

# **Turbo NAS**

## **User Manual (Version: 3.1.1)**

©Copyright 2009. QNAP Systems, Inc. All Rights Reserved.

Thank you for choosing QNAP products! This user manual provides detailed instructions of using the Turbo NAS. Please read carefully and start to enjoy the powerful functions of the Turbo NAS!

### **NOTE**

- “Turbo NAS” is hereafter referred to as “NAS”.
- This manual provides the description of all functions of the Turbo NAS. The product you purchased may not support certain functions dedicated to specific models.
- All features, functionality, and other product specifications are subject to change without prior notice or obligation.
- All brands and products names referred to are trademarks of their respective holders.

### **DISCLAIMER**

In no event shall the liability of QNAP Systems, Inc. (QNAP) exceed the price paid for the product from direct, indirect, special, incidental, or consequential software, or its documentation. QNAP makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. QNAP reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.



### **CAUTION**

1. Back up your system periodically to avoid any potential data loss. QNAP disclaims any responsibility of all sorts of data loss or recovery.
2. Should you return any components of the NAS package for refund or maintenance, make sure they are carefully packed for shipping. Any form of damages due to improper packaging will not be compensated.

# Table of Contents

<b>TABLE OF CONTENTS .....</b>	<b>3</b>
<b>SAFETY WARNINGS.....</b>	<b>6</b>
<b>CHAPTER 1 INSTALL THE NAS.....</b>	<b>7</b>
1.1 HARD DISK COMPATIBILITY LIST .....	7
1.2 CHECK SYSTEM STATUS .....	8
<b>CHAPTER 2 USE THE POWERFUL SERVICES OF NAS .....</b>	<b>11</b>
<b>CHAPTER 3 SERVER ADMINISTRATION .....</b>	<b>16</b>
3.1 SYSTEM ADMINISTRATION.....	18
3.1.1 General Settings .....	19
3.1.2 Network.....	21
3.1.2.1 TCP/IP .....	21
3.1.2.2 DDNS .....	26
3.1.3 Hardware .....	27
3.1.4 Security .....	29
3.1.4.1 Security Level.....	29
3.1.4.2 Network Access Protection.....	30
3.1.4.3 Import SSL Secure Certificate .....	31
3.1.5 Notification .....	32
3.1.5.1 Configure SMTP Server .....	32
3.1.5.2 Configure SMSC Server .....	33
3.1.5.3 Alert Notification.....	34
3.1.6 Power Management.....	35
3.1.7 Network Recycle Bin.....	36
3.1.8 Backup System Settings.....	37
3.1.9 System Logs .....	38
3.1.9.1 System Event Logs.....	38
3.1.9.2 System Connection Logs.....	39
3.1.9.3 On-line Users .....	40
3.1.9.4 Syslog .....	40
3.1.10 Firmware Update.....	41
3.1.11 System Reset .....	44
3.2 DISK MANAGEMENT.....	45
3.2.1 Volume Management.....	45

3.2.2	<i>RAID Management</i>	49
3.2.3	<i>HDD SMART</i>	50
3.2.4	<i>Encrypted File System</i>	51
3.2.5	<i>iSCSI</i>	52
3.2.6	<i>Virtual Disk</i>	53
3.3	ACCESS RIGHT MANAGEMENT	55
3.3.1	<i>Users</i>	55
3.3.2	<i>User Group</i>	57
3.3.3	<i>Share Folder</i>	58
3.3.4	<i>Quota</i>	59
3.4	NETWORK SERVICES	60
3.4.1	<i>Microsoft Networking</i>	60
3.4.2	<i>Apple Networking</i>	62
3.4.3	<i>NFS Service</i>	62
3.4.4	<i>FTP Service</i>	63
3.4.5	<i>Telnet/SSH</i>	65
3.4.6	<i>SNMP Settings</i>	66
3.4.7	<i>Web Server</i>	68
3.4.8	<i>Network Service Discovery</i>	69
3.4.8.1	<i>UPnP Discovery Service</i>	69
3.4.8.2	<i>Bonjour</i>	70
3.5	APPLICATIONS	71
3.5.1	<i>Web File Manager</i>	71
3.5.2	<i>Multimedia Station</i>	72
3.5.3	<i>Download Station</i>	72
3.5.4	<i>Surveillance Station</i>	73
3.5.5	<i>iTunes Service</i>	81
3.5.6	<i>UPnP Media Server</i>	84
3.5.7	<i>MySQL Server</i>	86
3.5.8	<i>QPKG Plugins</i>	88
3.6	BACKUP	90
3.6.1	<i>External Drive</i>	90
3.6.2	<i>USB One Touch Copy</i>	92
3.6.3	<i>Remote Replication (Disaster Recovery)</i>	93
3.7	EXTERNAL DEVICE	97
3.7.1	<i>External Storage Device</i>	97
3.7.2	<i>USB Printer</i>	98
3.7.2.1	<i>Windows XP Users</i>	99

3.7.2.2	<i>Windows Vista Users</i>	101
3.7.2.3	<i>Mac Users</i>	103
3.7.3	<i>UPS Settings</i>	107
3.8	SYSTEM STATUS	108
3.8.1	<i>System Information</i>	108
3.8.2	<i>System Service</i>	109
3.8.3	<i>Resource Monitor</i>	110
<b>CHAPTER 4 MULTIMEDIA STATION</b>		111
4.1	SHARE PHOTOS AND MULTIMEDIA FILES VIA THE WEB INTERFACE	111
<b>CHAPTER 5 DOWNLOAD STATION</b>		121
5.1	USE DOWNLOAD SOFTWARE QGET	130
<b>CHAPTER 6 WEB SERVER</b>		132
<b>CHAPTER 7 FTP SERVER</b>		136
<b>CHAPTER 8 WEB FILE MANAGER</b>		138
<b>CHAPTER 9 NETBAK REPLICATOR</b>		142
<b>CHAPTER 10 CONFIGURING AD AUTHENTICATION</b>		157
<b>CHAPTER 11 ACCESS NAS VIA LINUX OS</b>		162
<b>CHAPTER 12 NAS MAINTENANCE</b>		163
12.1	RESTART/ SHUT DOWN SERVER	163
12.2	RESET ADMINISTRATOR PASSWORD AND NETWORK SETTINGS	164
12.3	DISK FAILURE OR MALFUNCTION	165
12.4	POWER OUTAGE OR ABNORMAL SHUTDOWN	165
12.5	SYSTEM SOFTWARE ABNORMAL OPERATION	165
12.6	SYSTEM TEMPERATURE PROTECTION	165
<b>CHAPTER 13 RAID ABNORMAL OPERATION TROUBLESHOOTING</b>		166
<b>CHAPTER 14 USE THE LCD PANEL</b>		168
<b>TECHNICAL SUPPORT</b>		174
<b>GNU GENERAL PUBLIC LICENSE</b>		175

## **Safety Warnings**

1. The NAS can operate normally in the temperature of 0°C-40°C and relative humidity of 0%-95%. Please make sure the environment is well-ventilated.
2. The power cord and devices connected to the NAS must provide correct supply voltage (100W, 90-264V).
3. Do not place the NAS in direct sunlight or near chemicals. Make sure the temperature and humidity of the environment are in optimized level.
4. Unplug the power cord and all connected cables before cleaning. Wipe the NAS with a dry towel. Do not use chemical or aerosol to clean the NAS.
5. Do not place any objects on the NAS for the server's normal operation and to avoid overheating.
6. Use the flat head screws in the product package to lock the hard disks in the NAS when installing hard disks for proper operation.
7. Do not place the NAS near any liquid.
8. Do not place the NAS on any uneven surface to avoid falling off and damage.
9. Make sure the voltage is correct in your location when using the NAS. If you are not sure, please contact the distributor or the local power supply company.
10. Do not place any object on the power cord.
11. Do not attempt to repair your NAS in any occasions. Improper disassembly of the product may expose you to electric shock or other risks. For any enquiries, please contact the distributor.
12. The chassis NAS models should only be installed in the server room and maintained by the authorized server manager or IT administrator. The server room is locked by key or keycard access and only certified staff is allowed to enter the server room.

# **Chapter 1    Install the NAS**

For the information of the hardware installation, please refer to the "Quick Installation Guide" in the product package.

## **1.1    Hard Disk Compatibility List**

This product works with 2.5"/ 3.5" SATA hard disk drives from major hard disk brands. For the HDD compatibility list, please visit <http://www.qnap.com/>.



**QNAP disclaims any responsibility for product damage/  
malfunction or data loss/ recovery due to misuse or improper  
installation of hard disks in any occasions for any reasons.**

## 1.2 Check System Status

### LED Display & System Status Overview

LED	Colour	LED Status	Description
USB	Blue	Flashes blue every 0.5 sec	1) A USB device is detected 2) A USB device is being removed from the NAS 3) The USB device connected to the front USB port of the NAS is being accessed 4) The NAS data is being copied to the external USB device
		Blue	The USB device connected to the front USB port of the NAS is ready
		Off	The NAS has finished copying the data to the USB device connected to the front USB port
eSATA	Orange	Flashes	The eSATA device is being accessed
System Status	Red/ Green	Flashes green and red alternately every 0.5 sec	1) The hard drive on the NAS is being formatted 2) The NAS is being initialised 3) The system firmware is being updated 4) RAID rebuilding is in process 5) Online RAID Capacity Expansion is in process 6) Online RAID Level Migration is in process

		Red	<ul style="list-style-type: none"> <li>1) The hard drive is invalid</li> <li>2) The disk volume has reached its full capacity</li> <li>3) The disk volume is going to be full</li> <li>4) The system fan is out of function</li> <li>5) An error occurs when accessing (read/write) the disk data</li> <li>6) A bad sector is detected on the hard drive</li> <li>7) The NAS is in degraded read-only mode (2 member drives fail in a RAID 5 or RAID 6 configuration, the disk data can still be read)</li> <li>8) (Hardware self-test error)</li> </ul>
<b>System Status</b>	<b>Red/ Green</b>	Flashes red every 0.5 sec	The NAS is in degraded mode (one member drive fails in RAID 1, RAID 5 or RAID 6 configuration)
		Flashes green every 0.5 sec	<ul style="list-style-type: none"> <li>1) The NAS is starting up</li> <li>2) The NAS is not configured</li> <li>3) The hard drive is not formatted</li> </ul>
		Green	The NAS is ready
		Off	All the hard drives on the NAS are in standby mode
<b>HDD</b>	<b>Red/ Green</b>	Flashes red	The hard drive data is being accessed and a read/ write error occurs during the process
		Red	A hard drive read/ write error occurs
		Flashes green	The hard drive data is being accessed
		Green	The hard drive can be accessed
<b>LAN</b>	<b>Orange</b>	Orange	The NAS is connected to the network
		Flashes orange	The NAS is being accessed from the network

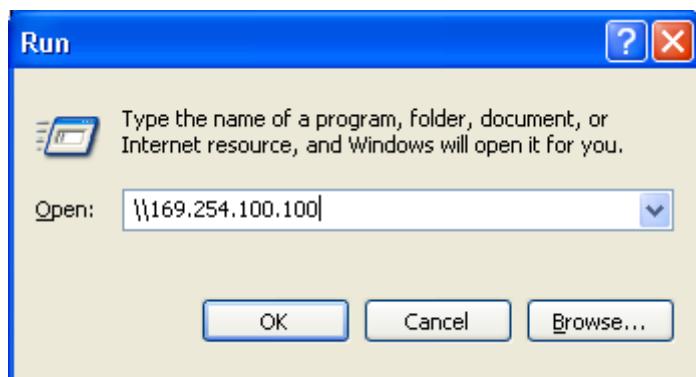
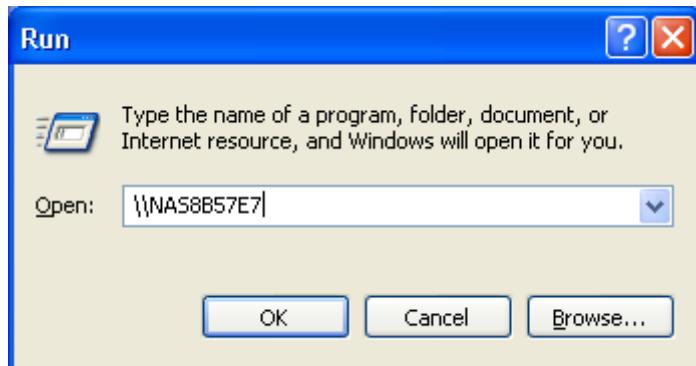
**Beep Alarm (beep alarm can be disabled in "System Tools" > "Hardware Settings")**

<b>Beep sound</b>	<b>No. of Times</b>	<b>Description</b>
Short beep (0.5 sec)	1	1) The NAS is starting up 2) The NAS is being shut down (software shutdown) 3) The user presses the reset button to reset the NAS 4) The system firmware has been updated
Short beep (0.5 sec)	3	The user tries to copy the NAS data to the external storage device from the front USB port, but the data cannot be copied.
Short beep (0.5 sec), long beep (1.5 sec)	3, every 5 min	The system fan is out of function
Long beep (1.5 sec)	2	1) The disk volume is going to be full 2) The disk volume has reached its full capacity 3) The hard drives on the NAS are in degraded mode 4) The user starts the HDD rebuilding process
	1	1) The NAS is turned off by force shutdown (hardware shutdown) 2) The NAS has been turned on successfully and is ready

## Chapter 2    Use the Powerful Services of NAS

### A. Use the network shares

1. You can access the network shares of the NAS by the following means:
  - a. Open My Network Places and find the workgroup of the NAS. If you cannot find the server, browse the whole network to search for the NAS. Double click the name of the NAS for connection.
  - b. Use Run function in Windows. Enter **\[NAS name]** or **\[NAS IP]** to access the share folders on the NAS.



2. Enter the default user name and password.

Default user name: **admin**  
Password: **admin**

3. You can upload files to the network shares.

## **B. Manage the NAS**

- Manage the NAS using web browser by Windows® or Mac

1. You can access the NAS web administration page by the following methods:
    - a. Use the Finder to find the NAS.
    - b. Open a web browser and enter **http://[NAS IP]:8080**

The default NAS IP is 169.254.100.100:8080. If you have configured the NAS to use DHCP, you can use the Finder to check the IP address of the NAS. Make sure the NAS is connected to the same subnet of your computer that runs the Finder. If you cannot search for the NAS IP, please try to connect the NAS to your computer directly and run the Finder again.

- When the administration page of the NAS is shown, click "ADMINISTRATION". Enter the user name and password to login.

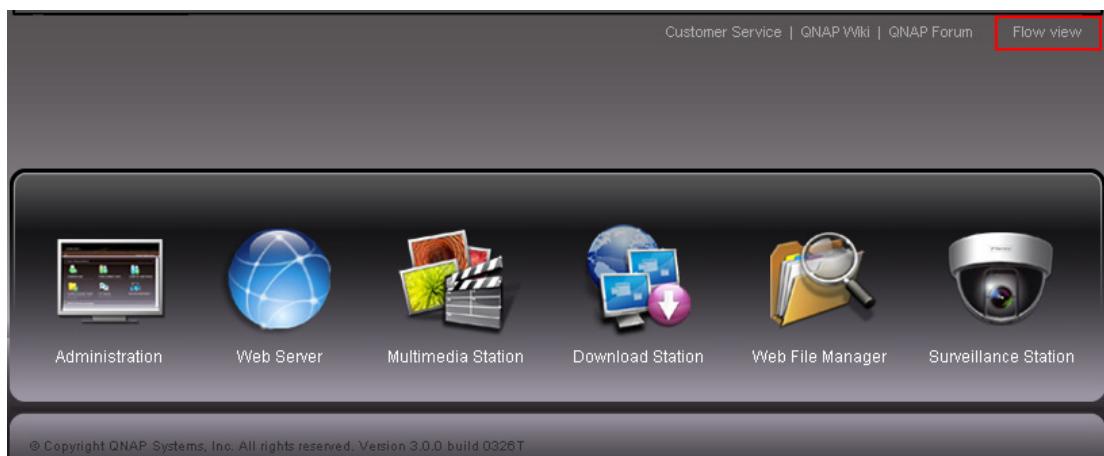
Default user name: admin

Password: admin



3. You can select to browse the NAS UI with Standard view or Flow view.

**Standard view:**



**Flow view:**



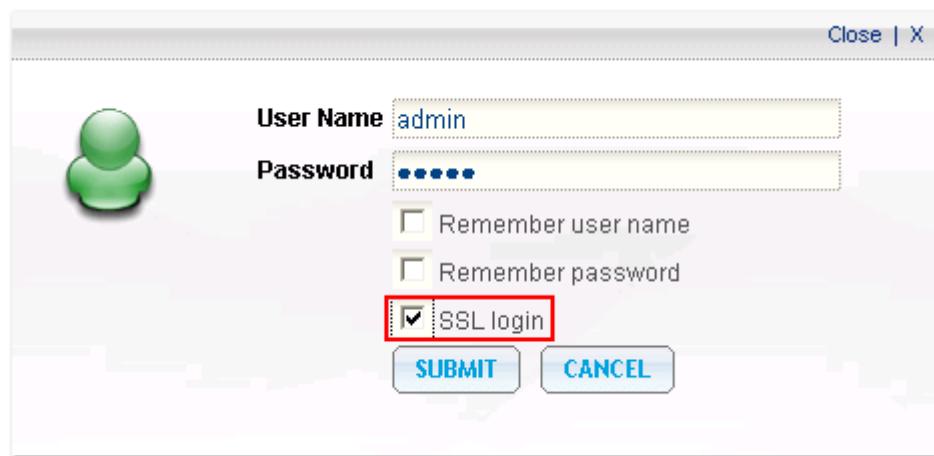
4. You can select the display language on the drop-down menu on the login page of the NAS or after you login the NAS.



A screenshot of the Synology NAS home page. At the top, there is a navigation bar with icons for "Web File Manager", "Multimedia Station", "Download Station", and "Surveillance Station". On the far right of the navigation bar is a "Welcome admin | Logout" link and a language selection dropdown set to "English". Below the navigation bar, there are two main sections: "Create Multiple Users" and "Create a User Group". Each section has an icon, a title, and a brief description. To the right of these sections is another language selection dropdown, identical to the one at the top, listing the same 14 languages. At the bottom left, there is a "Service" section with an icon and a "Remote Replication" section with an icon.

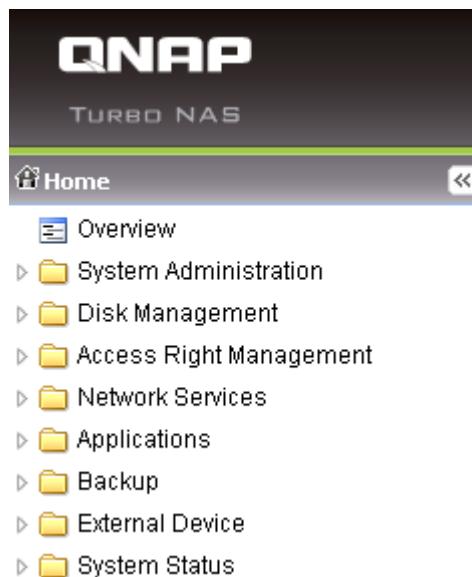
5. The NAS supports SSL secure login which enables you to configure and manage the server by encrypted transfer. To use this function, check the box "SSL login" on the administration page and login the server.

**Note:** If your NAS is placed behind an NAT gateway and you want to access the NAS by secure login from the Internet, you must open the port 443 on your NAT and forward this port to LAN IP of the NAS.

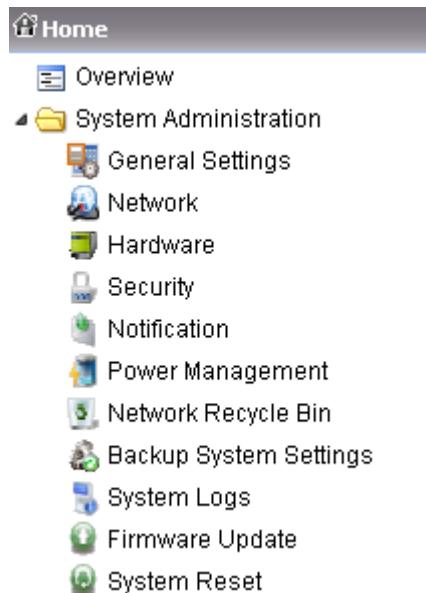


## Chapter 3 Server Administration

There are 8 main sections in server administration.



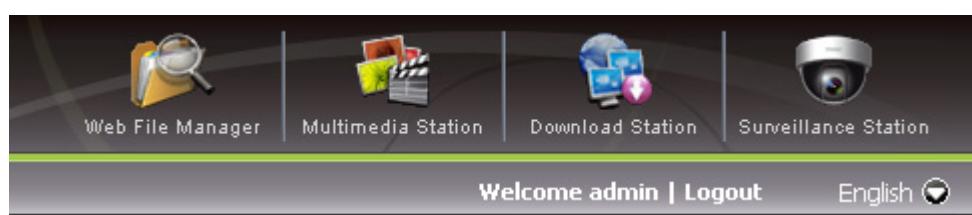
Click on the triangle icon next to the section name to expand the tree and view the items listed under each section.



To access the services such as Web File Manager, Download Station, Multimedia Station, and Surveillance Station, you can select the services from the drop-down menu or click the icons on the login page.

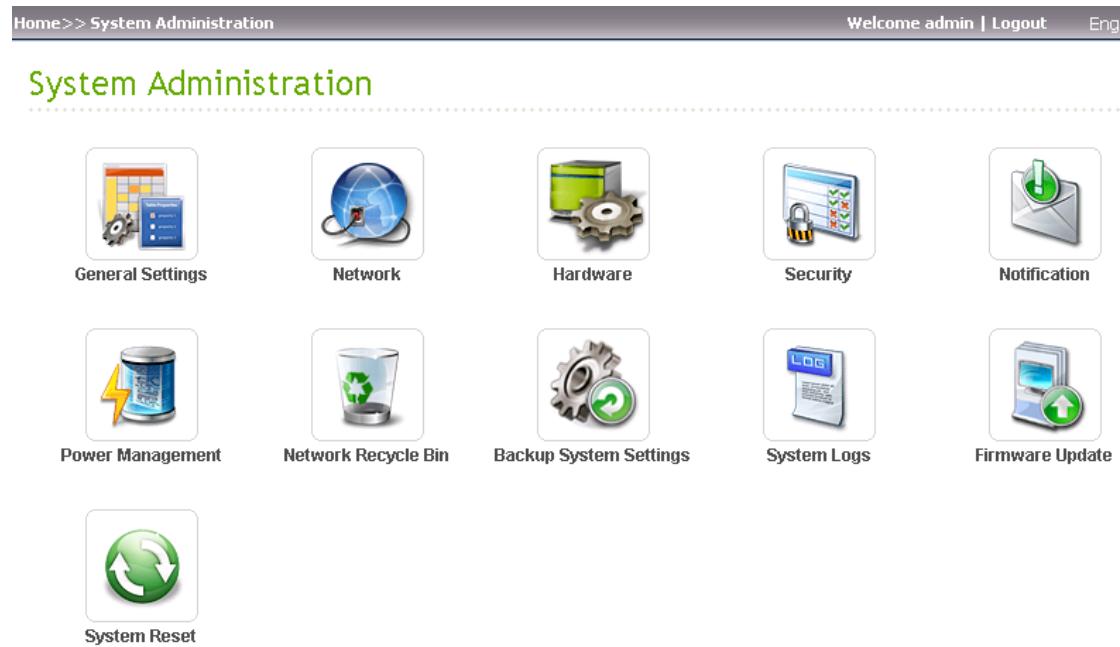


After you login the NAS, you can click the icons on top of the page to access the services.



## 3.1 System Administration

You can configure the general system settings, network settings, and hardware settings, update the firmware, etc. in this section.



### 3.1.1 General Settings

The screenshot shows the 'General Settings' page with three main sections: 'System Administration', 'Date and Time', and 'Language'.  
**System Administration:** Contains fields for 'Server Name' (NAS8C3E6F) and 'System Port' (8080).  
**Date and Time:** Includes a dropdown for 'Time Zone' (GMT+08:00 Taipei), a date/time picker, and checkboxes for 'Synchronize with an internet time server automatically' (set to pool.ntp.org) and 'Set the server time the same as your computer time'.  
**Language:** Shows 'Filename Encoding' set to English.  
At the bottom right is an 'APPLY' button.

#### ➤ System Administration

Enter the name of the NAS. The server name can be 14 characters long at maximum, which supports alphabets, numbers, and hyphen (-). The server does not accept names with space, period (.), or names in pure number.

Assign a port for the system management. The default port is 8080. The services which use this port include: System Management, Web File Manager, Multimedia Station, and Download Station.

#### ➤ Date and Time

Set the date, time, and time zone according to your location. If the settings are incorrect, the following problems may occur:

- When using a web browser to access the server or save a file, the display time of the action will be incorrect.
- The time of event log displayed will be inconsistent with the actual time when an action occurs.

✓ **Synchronize with an Internet time server automatically**

You can enable this option to update the date and time of the system automatically with specified NTP (Network Time Protocol) server. Enter the IP address or domain name of the NTP server, e.g. time.nist.gov, time.windows.com. Then enter the time interval for adjusting the time.

**Note:** The first time you enable NTP server, it may take several minutes for time synchronization before the time is correctly adjusted.

➤ **Language**

Select the language the NAS uses to display files and directories.

**Note:** All the files and directories on the NAS will be created using Unicode encoding. If your FTP clients or the OS of your PC does not support Unicode, e.g. Windows® 95/98/ME, select the language the same as your OS here in order to view the files and directories on the server properly.

## 3.1.2 Network

### 3.1.2.1 TCP/IP

Click  to edit the network settings.

**Network**

**TCP / IP** **DDNS**

**IP Address**

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
Ethernet 1	No	172.17.21.123	255.255.254.0	172.17.20.1	00:08:9B:B9:27:B1	1000Mbps	1500		
Ethernet 2	Yes	169.254.100.100	255.255.0.0	0.0.0.0	00:08:9B:B9:27:B0	--	0		

**Port Trunking**

Port Trunking provides network load balancing and fault tolerance by combining two Ethernet interfaces into one to increase the bandwidth beyond the limits of any one single interface at the same time offers the redundancy for higher availability when both interfaces are connected to the same switch that supports 'Port Trunking'.

Enable Network Port Trunking

Select the port trunking mode from below. Please note that incompatible mode settings might cause the network interface to hang or affect the overall performance. For more information, please click [here](#).

Balance-rr (Round-Robin)

**DNS Server:**

Primary DNS Server: 172.17.21.121

Secondary DNS Server: 0.0.0.0

**APPLY**

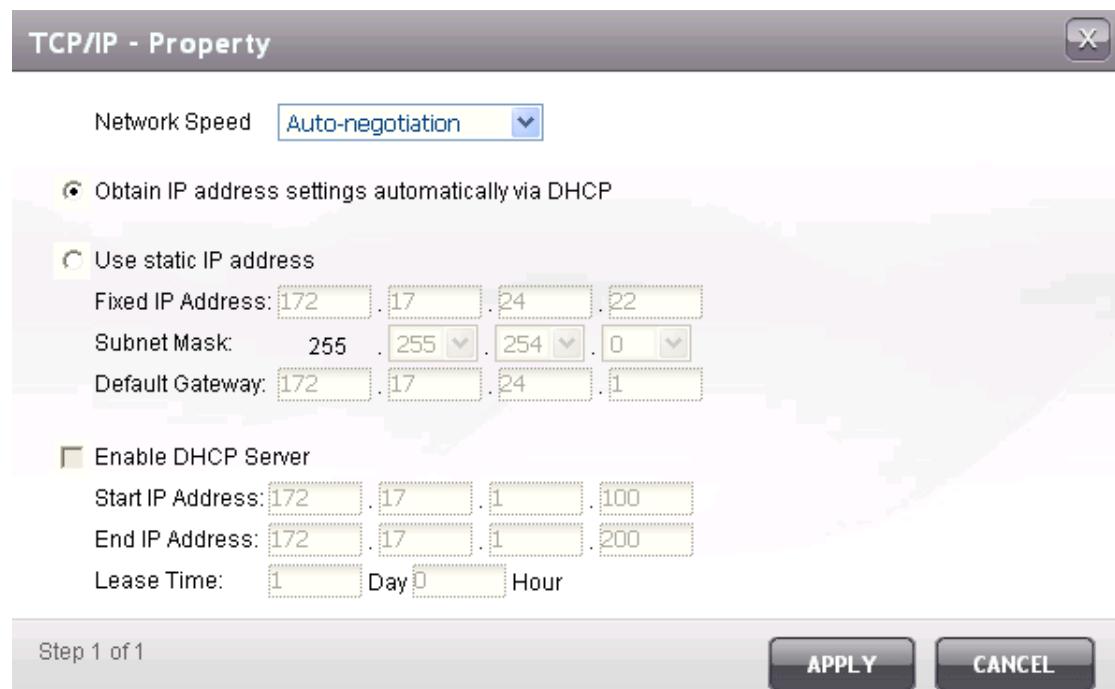
You can select one of the following two methods to configure the TCP/IP settings of the NAS.

- **Obtain IP address settings automatically via DHCP**

If your network supports DHCP, the NAS will use DHCP protocol to retrieve the IP address and related information automatically.

- **Use static IP address**

To use fixed IP address for network connection, enter fixed IP address, subnet mask, and default gateway.



## **Enable DHCP Server**

If no DHCP is available in the LAN where the NAS locates, you can enable this function to enable the NAS as a DHCP server and allocate dynamic IP address to DHCP clients in LAN.

You can set the range of IP addresses allocated by DHCP server and the lease time. Lease time refers to time that IP address is leased to the clients by DHCP server. When the time expires, the client has to acquire an IP address again.

For example, to establish a DLNA network, and share the multimedia files on the NAS to DLNA digital media player via UPnP while there is no NAT gateway that supports DHCP server, you can enable DHCP server of the NAS. The NAS will allocate dynamic IP address to DMP or other clients automatically and set up a local network.

**Note:** If there is an existing DHCP server in your LAN, do not enable this function. Otherwise, there will be IP address allocation and network access errors.

## **Port Trunking**

\* Applicable to models with two LAN ports only.

Port Trunking provides network load balancing and fault tolerance by combining two Ethernet interfaces into one to increase the bandwidth beyond the limits of any one single interface at the same time offers the redundancy for higher availability when both interfaces are connected to the same switch that supports 'Port Trunking'.

Field	Description
Balance-rr (Round-Robin)	The packets are transmitted in sequential order from the first available slave to the last. This mode provides load balancing and fault tolerance.
Active Backup	Only one active slave is used to transmit packets. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.
Balance XOR	The packets are transmitted based on the hash policy. The default policy is a simple [(source MAC address

	XOR'd with destination MAC address) modulo slave count]. Alternate transmit policies may be selected via the xmit_hash_policy option. This mode provides load balancing and fault tolerance.
Broadcast	The packets are transmitted on all slave interfaces. This mode provides fault tolerance.
IEEE 802.3ad	The Ethernet interfaces are aggregated in a group and each slave shares the same speed. This mode provides load balancing and fault tolerance. Make sure the switch supports IEEE 802.3ad standard and the correct LACP mode is configured.
Balance-tlb (Adaptive Transmit Load Balancing)	Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave. This mode provides load balancing and fault tolerance.
Balance-alb (Adaptive Load Balancing)	Include balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The receive load balancing is achieved by ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware address for the server. This mode provides load balancing and fault tolerance.

### DNS Server

- **Primary DNS Server:** Enter the IP address of primary DNS server that provides DNS service for the NAS in external network.
- **Secondary DNS Server:** Enter the IP address of secondary DNS server that provides DNS service for the NAS in external network.

**Note:**

1. Please contact your ISP or network administrator for the IP address of primary and secondary DNS servers. When the NAS plays the role as a terminal and needs to perform independent connection, e.g. BT download, you must enter at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.
2. If you select to obtain IP address via DHCP, there is no need to configure the primary and secondary DNS servers. You can enter "0.0.0.0" in the settings.

### Jumbo Frame Settings (MTU)

"Jumbo Frames" refer to Ethernet frames that are larger than 1500 bytes. It is designed to enhance Ethernet networking throughput and reduce the CPU utilization of large file transfers by enabling more efficient larger payloads per packet.

Maximum Transmission Unit (MTU) refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can transmit.

The NAS uses standard Ethernet frames: **1500 bytes** by default. If your network appliances support Jumbo Frame setting, select the appropriate MTU value for your network environment. The NAS supports 4074, 7418, and 9000 bytes for MTU.

**Note:** Jumbo Frame setting is valid in Gigabit network environment only. Besides, all network appliances connected must enable Jumbo Frame and use the same MTU value.

### 3.1.2.2 DDNS

After enabling DDNS Service, you can connect to this server by domain name.

Enable Dynamic DNS Service

Select DDNS server:

Enter the account information you registered with the DDNS provider

User Name:

Password:

Host Name:

Check the External IP Address Automatically

(External IP: 219.85.63.13)

To set up a server on the Internet and enable users to access it easily, a fixed and easy-to-remember host name is often required. However, if ISP provides only dynamic IP address, the IP address of the server will change from time to time and is difficult to recall. You can enable DDNS service to solve the problem.

After enabling DDNS service of the NAS, whenever the NAS restarts or the IP address is changed, the NAS will notify the DDNS provider immediately to record the new IP address. When the user tries to connect the NAS via the host name, DDNS will transfer the recorded IP address to the user.

The NAS supports the DDNS providers: members.dyndns.org, update.ods.org, members.dhs.org, www.dyns.cx, www.3322.org, www.no-ip.com.

For the information of setting up DDNS and port forwarding on the NAS, please refer to the online tutorial: [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

### 3.1.3 Hardware

You can enable or disable the hardware functions of the NAS.

The screenshot shows the 'Hardware' configuration page. At the top, there's a header 'Hardware'. Below it, under 'Hardware', there are four checkboxes: 'Enable configuration reset switch' (checked), 'Enable hard disk standby mode (if no access within  minutes, Status LED will be off)' (checked), 'Enable light signal alert when the free size of disk is less than the value:  MB' (checked), and 'Enable alarm buzzer (beep sound for error and warning alert)' (checked). Below this is a section titled 'Smart Fan Configuration' with a dropdown menu set to 'Enable Smart Fan (recommended)'. It contains two radio button options: one for 'When ALL the following temperature readings are met the fan will rotate at low speed' (selected) with sub-options for system, CPU, and hard drive temperatures; and another for 'When ANY the following temperature readings are met the fan will rotate at high speed' with sub-options for system, CPU, and hard drive temperatures. There are also three checkboxes for 'Self-defined temperature': one for stopping rotation at 25°C, one for low speed at 35°C, and one for high speed at 45°C. At the bottom right is an 'APPLY' button.

- Enable configuration reset switch

You can press the reset button for 3 seconds to reset the administrator password and system settings to default.

- Enable hard disk standby mode

When this function is enabled, hard disk will go to standby mode if there is no access within the specified period.

- Enable light signal alert when the free size of SATA disk is less than the value:  
The Status LED indicator flashes red and green when this function is enabled and the free space of the SATA disk is less than the value. The range of the value is 1-51200 MB.

- Enable alarm buzzer

Enable this option. The system will sound when an error occurs.

- Smart Fan configuration

- (i) Enable smart fan (recommended)

Select to use the default smart fan settings or define the settings manually.

When the system default settings are selected, the fan rotation speed is

automatically adjusted when the server temperature, CPU temperature, and hard drive temperature meet the criteria. It is recommended to enable this option.

#### – Smart Fan Configuration

Fan Rotation Speed Settings: **Enable Smart Fan (recommended)** 

- When ALL the following temperature readings are met the fan will rotate at low speed:

- The system temperature is lower than 47°C(117°F).
- The CPU temperature is lower than 54°C(129°F).
- The hard drive temperature is lower than 48°C(118°F).

- When ANY the following temperature readings are met the fan will rotate at high speed:

- The system temperature is higher than or equal to 53°C(127°F).
- The CPU temperature is higher than or equal to 62°C(144°F).
- The hard drive temperature is higher than or equal to 54°C(129°F).

- Self-defined temperature:

When the system temperature is lower than   °C  , stop fan rotation.

When the system temperature is lower than   °C  , rotate at low speed.

When the system temperature is higher than   °C  , rotate at high speed.

#### (ii) Set fan rotation speed manually

By manually setting the fan rotation speed, the fan rotates at the defined speed continuously.

#### – Smart Fan Configuration

Fan Rotation Speed Settings: **Set fan rotation speed manually** 

- Low speed

- Medium speed

- High speed

### **3.1.4 Security**

#### **3.1.4.1 Security Level**

Enter the IP address or network from which the connections to this server are allowed or rejected. When the connection of a host server is denied, all protocols of that server are not allowed to access the local server.

After changing the settings, click "Apply" to save the changes. The network services will be restarted and current connections to the server will be disconnected.

**Security**

**SECURITY LEVEL**   **NETWORK ACCESS PROTECTION**   **IMPORT SSL SECURE CERTIFICATE**

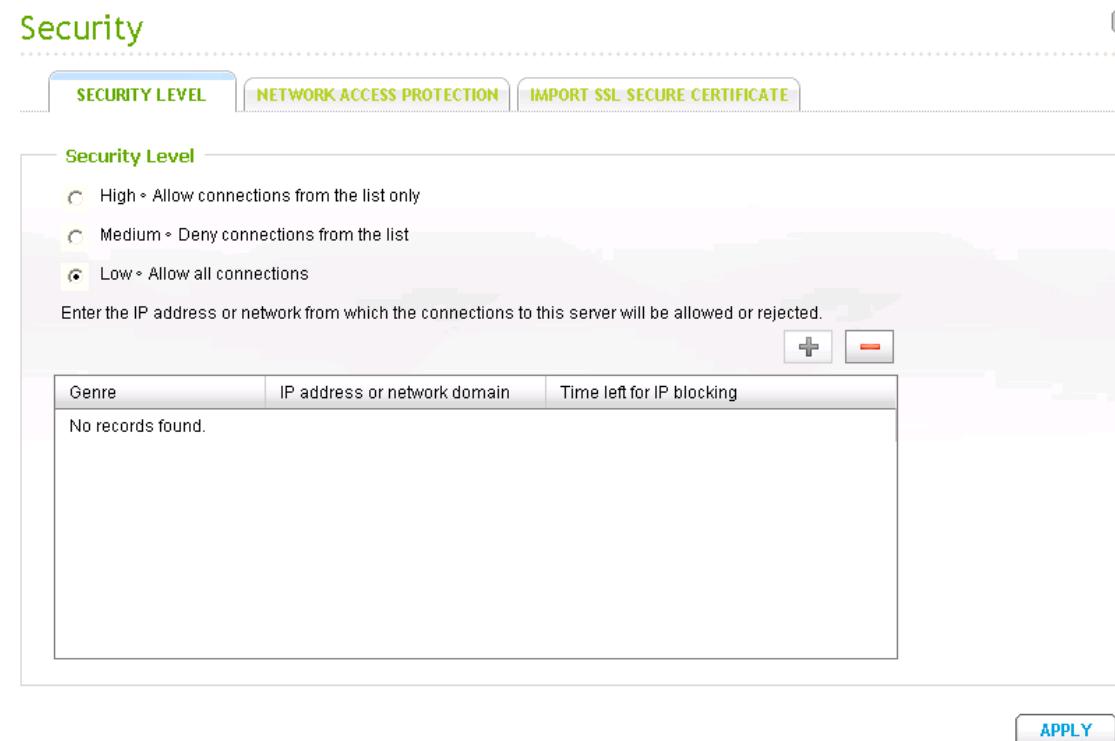
**Security Level**

High ▾ Allow connections from the list only  
 Medium ▾ Deny connections from the list  
 Low ▾ Allow all connections

Enter the IP address or network from which the connections to this server will be allowed or rejected.

Genre	IP address or network domain	Time left for IP blocking
No records found.		

**APPLY**



### **3.1.4.2 Network Access Protection**

The network access protection enhances the security of the system and prevents unwanted intrusion. You can select to block the IP for a certain period of time or forever if the IP fails to login the server from a particular connection method.

The screenshot shows a software interface for managing network access protection. At the top, there are three tabs: "SECURITY LEVEL" (disabled), "NETWORK ACCESS PROTECTION" (selected and highlighted in blue), and "IMPORT SSL SECURE CERTIFICATE". Below the tabs, a section titled "Network Access Protection" contains a list of connection types with their respective settings. An "Enable network access connection" checkbox is checked. Underneath it, checkboxes are present for various protocols, each with a dropdown menu for time intervals. A large "APPLY" button is located at the bottom right of the configuration area.

Protocol	Time Interval (After Unsuccessful Attempts)	Block Duration (IP Block)
SSH	10 minutes	10 time(s) / 5 minutes
Telnet	10 minutes	10 time(s) / 5 minutes
HTTP(S)	10 minutes	10 time(s) / 5 minutes
FTP	10 minutes	10 time(s) / 5 minutes
SAMBA	10 minutes	10 time(s) / 5 minutes
AFP	10 minutes	10 time(s) / 5 minutes

### **3.1.4.3 Import SSL Secure Certificate**

The Secure Socket Layer (SSL) is a protocol for encrypted communication between web servers and browsers for secure data transfer. You can upload a secure certificate issued by a trusted provider. After you have uploaded a secure certificate, you can access the administration interface by SSL connection and there will not be any alert or error message. The system supports X.509 certificate and private key only.

The screenshot shows a user interface for importing an SSL certificate. At the top, there are three tabs: 'SECURITY LEVEL', 'NETWORK ACCESS PROTECTION', and 'IMPORT SSL SECURE CERTIFICATE'. The third tab is highlighted. Below the tabs, the title 'Import SSL Secure Certificate' is displayed. A descriptive text states: 'You can upload a secure certificate issued by a trusted provider. After you have uploaded a secure certificate successfully, you can access the administration interface by SSL connection and there will not be any alert or error message.' Another note says: 'If you upload an incorrect secure certificate, you may not be able to login the server via SSL. To resolve the problem, you can restore the secure certificate to default and access the system again.' The status is shown as 'Status: Default secure certificate being used'. There are two main input fields: one for 'Certificate' (labeled 'Please enter a certificate in X.509PEM format below.') and one for 'Private Key' (labeled 'Please enter a certificate or private key in X.509PEM format below.'). Each field has a 'View sample' link. At the bottom right are 'CLEAR' and 'UPLOAD' buttons.

### 3.1.5 Notification

Notification

CONFIGURE SMTP SERVER    CONFIGURE SMSC SERVER    ALERT NOTIFICATION

Configure SMTP Server

SMTP Server: mail  
Port Number: 25  
Sender: tester

Enable SMTP Authentication  
User Name:   
Password:

Use SSL/TLS secure connection

APPLY



#### 3.1.5.1 Configure SMTP Server

Configure the SMTP server for outgoing mails of this server. If your mail server requires SMTP authentication, enter the user name and password for the mail server.

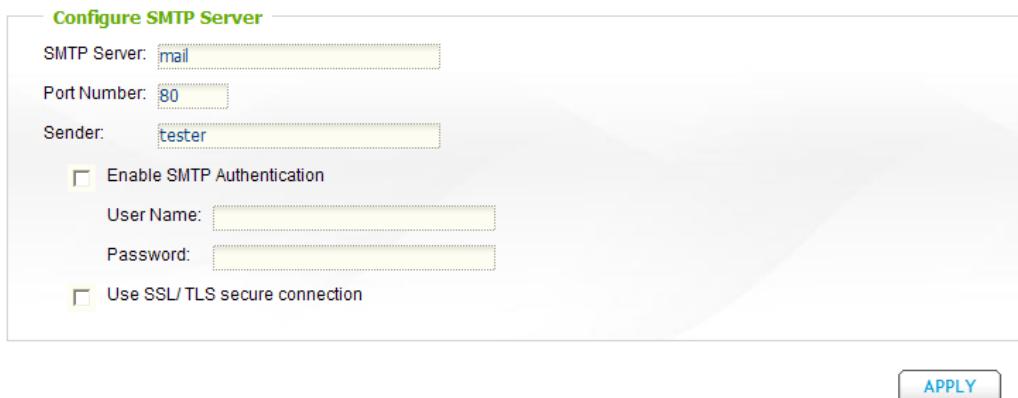
Configure SMTP Server

SMTP Server: mail  
Port Number: 80  
Sender: tester

Enable SMTP Authentication  
User Name:   
Password:

Use SSL/TLS secure connection

APPLY



### **3.1.5.2      Configure SMSC Server**

You can configure the SMS server settings to send SMS messages from the NAS. The default SMS service provider is Clickatell. You may also add your own SMS service provider by selecting “Add SMS Provider” on the drop down menu.

When you select “Add SMS service provider”, you need to enter the name of the SMS provider and the URL template text.

**Note:** You will not be able to receive the SMS properly if the URL template text entered does not follow your SMS service provider’s standard.

**Configure SMSC Server**

You can configure the SMSC settings to send instant system alerts via the SMS service provided by the SMS provider.

SMS Service Provider  http://www.clickatell.com

Enable SSL Connection

SSL Port:

SMS Server Login Name:

SMS Server Login Password:

SMS Server API\_ID:

### **3.1.5.3 Alert Notification**

You can configure to receive instant SMS or email alert when a system error or warning occurs. Enter the email address and mobile phone number to receive the alerts. Make sure you have entered the correct SMTP server and the SMSC server settings. If you do not want to receive any alerts, select "No alert" for both settings.

For the online tutorial, please visit [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

The screenshot shows a web-based configuration interface for alert notifications. At the top, there are three tabs: "CONFIGURE SMTP SERVER" (disabled), "CONFIGURE SMSC SERVER" (disabled), and "ALERT NOTIFICATION" (selected).  
  
**Alert Notification**  
When a system event occurs, an alert email will be sent automatically.  
Send system error alert by:  (dropdown menu)  
Send system warning alert by:  (dropdown menu)  
  
**E-mail Notification**  
E-mail address 1:   
E-mail address 2:   
  
  
**Note:** The SMTP server must be configured first for alert mail delivery.  
  
**SMS Notification Settings**  
Country Code:  (dropdown menu)  
Cell Phone No. 1: +93   
Cell Phone No. 2: +93   
  
  
**Note:** You must configure the SMSC server to be able to send SMS notification properly.

### 3.1.6 Power Management

This section enables you to restart or shut down the server immediately, define the behavior of the server when the power resumes after a power outage, and set schedule for automatic system power on/ off/ restart.

Wake on LAN: Enable this option to power on the NAS remotely by Wake on LAN. This function is applicable to some models only. Please refer to the comparison table for more details:

[http://www.qnap.com/images/products/comparison/Comparison\\_NAS.html](http://www.qnap.com/images/products/comparison/Comparison_NAS.html)

You can select every day, weekdays, weekend, or any days of the week and set the time for automatic system power on, power off, or restart. Weekdays stand for Monday to Friday; weekend stands for Saturday and Sunday. Up to 15 schedules can be set.

The screenshot shows the Power Management settings page with the following sections:

- Restart/ Shutdown:** Allows immediate system restart or shutdown. It includes a button to execute the action.
- Configure Wake on LAN:** Offers options to enable or disable the feature.
- When the AC power resumes:** Provides choices for how the server should respond upon power restoration.
- Set power on/ power off/ restart schedule:** Allows setting up to 15 scheduled events. The table below shows three examples of scheduled actions:

Action	Day	Hour	Minute
Turn on the server	Daily	16	5
Turn on the server	Daily	16	10
Turn on the server	Daily	16	20

An **APPLY** button is located at the bottom right of the configuration area.

### 3.1.7 Network Recycle Bin

This function enables the files deleted on the shares of the NAS to be removed to Network Recycle Bin to reserve the files temporarily. To enable this function, check the box "Enable Network Recycle Bin" and click "Apply". The system will create a network share "Network Recycle Bin" automatically.

To delete all the files in network recycle bin, click "Empty Network Recycle Bin".

**Network Recycle Bin**

Network Recycle Bin

After enabling Network Recycle Bin, all the deleted files on the network folders of the NAS are moved to the "Network Recycle Bin" network folder.

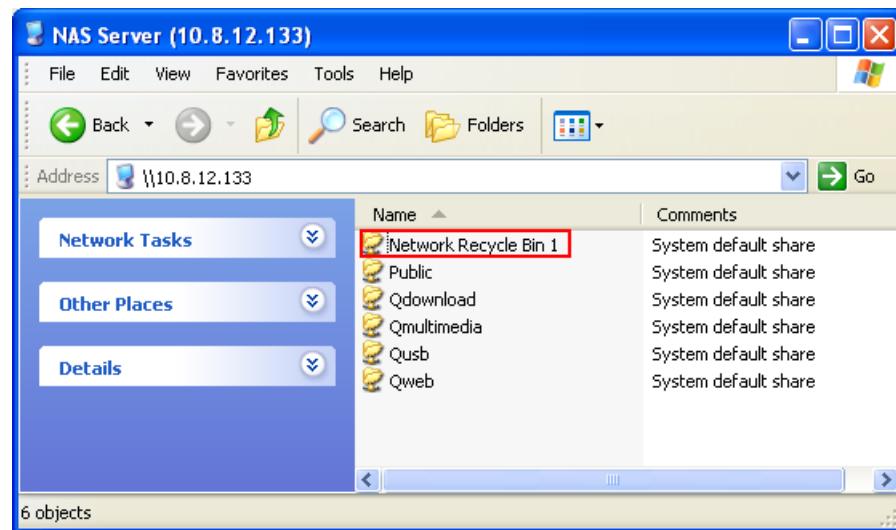
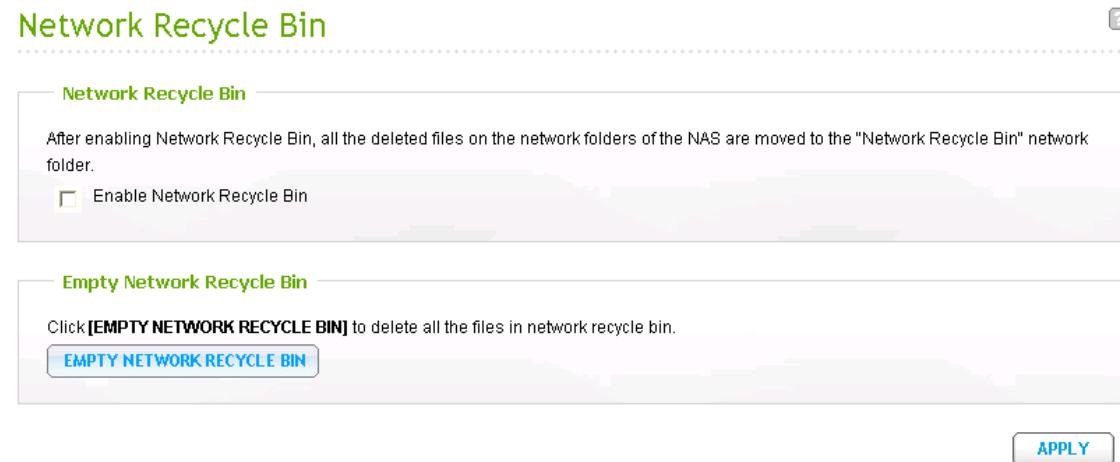
Enable Network Recycle Bin

Empty Network Recycle Bin

Click [EMPTY NETWORK RECYCLE BIN] to delete all the files in network recycle bin.

**EMPTY NETWORK RECYCLE BIN**

**APPLY**



### 3.1.8 Backup System Settings

- To backup all the settings, including the user accounts, server name and network configuration etc., click “Backup” and select to open or save the setting file.
- To restore all the settings, click “Browse” to select a previously saved setting file and click “Restore”.

#### Backup System Settings

##### Backup System Settings

To backup all settings, including user accounts, server name and network configuration etc., click [BACKUP] and select to open or save the setting file.

**BACKUP**

##### Restore System Settings

To restore all settings, click [Browse...] to select a previously saved setting file and click [RESTORE] to confirm.

**RESTORE**

### 3.1.9 System Logs

#### 3.1.9.1 System Event Logs

The NAS can store 10,000 recent event logs, including warning, error, and information messages. In case of system malfunction, event logs can be retrieved to analyze system problems.

**Tip:** You can right click a log and delete the record.

The screenshot shows a web-based interface titled "System Logs". At the top, there are four tabs: "SYSTEM EVENT LOGS" (which is selected and highlighted in blue), "SYSTEM CONNECTION LOGS", "ON-LINE USERS", and "SYSLOG". Below the tabs is a toolbar with buttons for "All events" (with a dropdown menu), "Clear", and "Save". A table displays 22 system event logs. The columns are: Type, Date, Time, Users, Source IP, Computer name, and Content. The "Content" column contains log messages such as "[Web Server] started successfully.", "[Single Disk Volume: Drive 1] Recovering journal.", and "System was shut down on Thu May 14 18:35:01 CST 2009.". One specific log entry for May 15, 2009, at 18:05:33 has a context menu open with the option "Delete this record". At the bottom of the table, there is a message stating "There are 22 events. Displays 10 records per page." followed by a page navigation bar with icons for back, forward, and search.

Type	Date	Time	Users	Source IP	Computer name	Content
Info	2009-05-15	18:05:33			localhost	[Web Server] started successfully.
Info	2009-05-15	11:18:16	System	127.0.0.1	localhost	[Single Disk Volume: Drive 1] Recovering journal.
Info	2009-05-15	11:18:08	System	127.0.0.1	localhost	System started.
Info	2009-05-14	18:35:01	System	127.0.0.1	localhost	System was shut down on Thu May 14 18:35:01 CST 2009.
Info	2009-05-14	18:08:43	System	127.0.0.1	---	Disabled iTunes password; iTunes service still in use.
Info	2009-05-14	16:49:12	System	10.8.10.7	---	Copy out: Backup configuration was change to [Do not backup].
Info	2009-05-13	09:50:44	System	127.0.0.1	localhost	System started.
Info	2009-05-12	20:02:02	System	127.0.0.1	localhost	System was shut down on Tue May 12 20:02:02 CST 2009.
Info	2009-05-12	16:57:53	System	127.0.0.1	localhost	[Single Disk Volume: Drive 1] Recovering journal.
Info	2009-05-12	16:57:45	System	127.0.0.1	localhost	System started.

### 3.1.9.2 System Connection Logs

The system supports logging HTTP, FTP, Telnet, SSH, AFP, NFS, SAMBA, and iSCSI connections. Click "Options" to select the connection type to be logged. The file transfer performance can be slightly affected by enabling the event logging.

**Tip:** You can right click the log on the list of connection logs and select to delete the record or add the IP to banned list and select how long the IP should be banned.

A screenshot of a software interface titled "SYSTEM CONNECTION LOGS". At the top, there are tabs for "SYSTEM EVENT LOGS", "SYSTEM CONNECTION LOGS" (which is selected), "ON-LINE USERS", and "SYSLOG". Below the tabs are several buttons: "All events" (with a dropdown arrow), "Options", "Stop logging", "Clear", and "Save". A table displays a single log entry:

Type	Date	Time	Users	Source IP	Computer name	Connection type	Accessed resources	Action
①	2009-06-08	16:35:06	admin	172.17.24.40	---	SSH	---	Login OK

Below the table, a message says "There is 1 event. Displays 10". A context menu is open over the first log entry, showing options: "Delete this record" and "Add to the block list". At the bottom right, there are navigation icons and a page number "1 / 1".

Archive logs: Enable this option to archive the connection logs. The system generates a csv file automatically and saves it to a specified folder when the number of logs reaches the upper limit.

A screenshot of a configuration dialog titled "Connection Type". It contains the following text: "Select the connection type to be logged." Below this are several checkboxes:

<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> FTP	<input checked="" type="checkbox"/> Telnet	<input checked="" type="checkbox"/> SSH
<input type="checkbox"/> AFP	<input checked="" type="checkbox"/> SAMBA	<input type="checkbox"/> iSCSI	

Below the checkboxes is a checkbox labeled "When the number of logs reaches 10,000, archive the connection logs and save the file in the folder:" followed by a dropdown menu containing "Qdownload". At the bottom of the dialog are "APPLY" and "CANCEL" buttons.

### **3.1.9.3 On-line Users**

The information of the on-line users accessing the system via networking services is shown in this page.

**Tip:** You can right click a log and select to disconnect the IP connection and/or add the IP to the block list.

Type	Login date	Login time	Users	Source IP	Computer name	Connection type	Accessed resource
user	2009-06-08	16:26:06	admin	10.8.10.122	---	HTTP	Administration
user	2009-06-08	16:26:06	admin	172.17.24.40	---	SSH	---

There are 2 events.

- 
- 
- 

### **3.1.9.4 Syslog**

Syslog is a standard for forwarding log messages in an IP network. You can enable this option to save the event logs and connection logs to a remote syslog server.

**Syslog Settings**

Enable syslog  
You can enable this option to save the event logs and connection logs to a remote syslog server.

Syslog Server IP:

UDP Port:

Select the logs to record

System Event Logs

System Connection Logs (You must enable system connection logs to use this option.)

### 3.1.10 Firmware Update

#### Firmware Update

**Firmware Update**

Current firmware version: 3.1.0 Build 0608T

Before updating system firmware, please make sure the product model and firmware version are correct. Follow the steps below to update firmware:

1. Download the release notes of the same version as the firmware from QNAP website <http://www.qnap.com>. Read the release notes carefully to make sure you need to update the firmware.
2. Before updating system firmware, back up all disk data on the server to avoid any potential data loss during system update.
3. Click the [Browse...] button to select the correct firmware image for system update. Click the [UPDATE SYSTEM] button to update the firmware.

**Note:** System update may take tens of seconds to several minutes to complete depending on the network connection status, please wait patiently. The system will inform you when system update is completed.

**Note:** If the system is running properly, you do not need to update the firmware.

Before updating the system firmware, make sure the product model and firmware version are correct. Follow the steps below to update firmware:

**Step 1:** Download the release notes of the same version as the firmware from QNAP website <http://www.qnap.com>. Read the release notes carefully to make sure you need to upgrade the firmware.

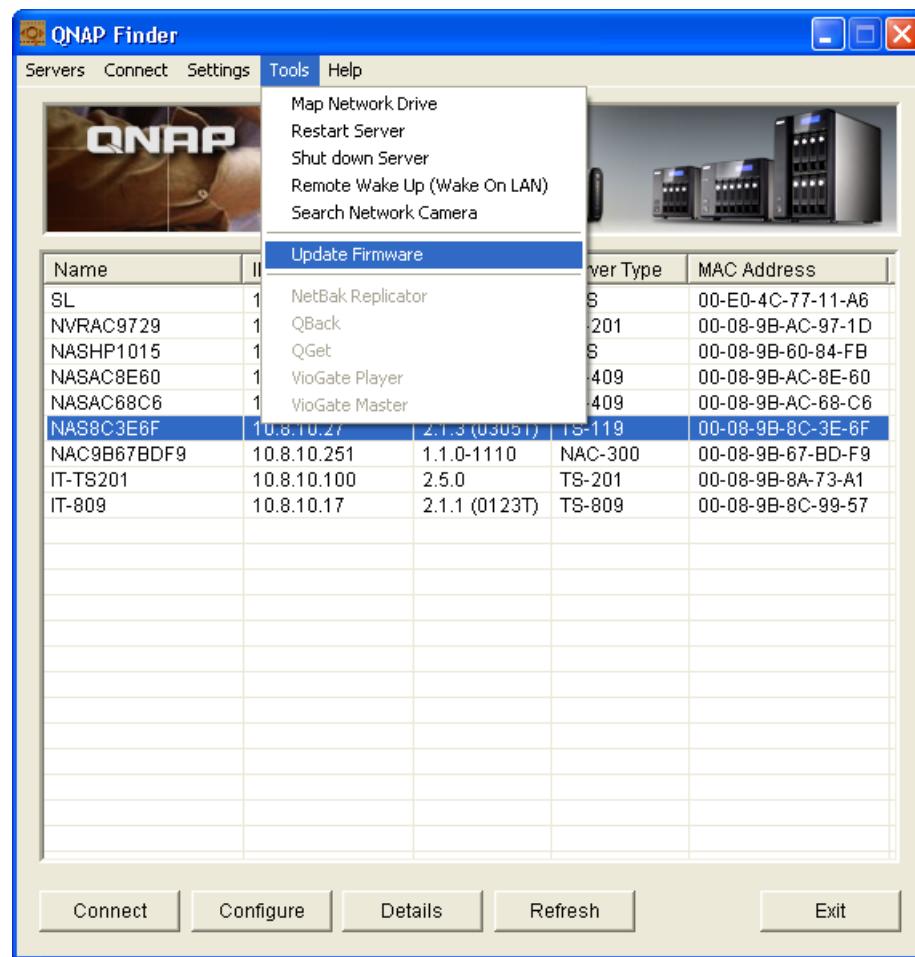
**Step 2:** Before upgrading system firmware, back up all disk data on the server to avoid any potential data loss during system update.

**Step 3:** Click "Browse" to select the correct firmware image for system update. Click "Update System" to update the firmware.

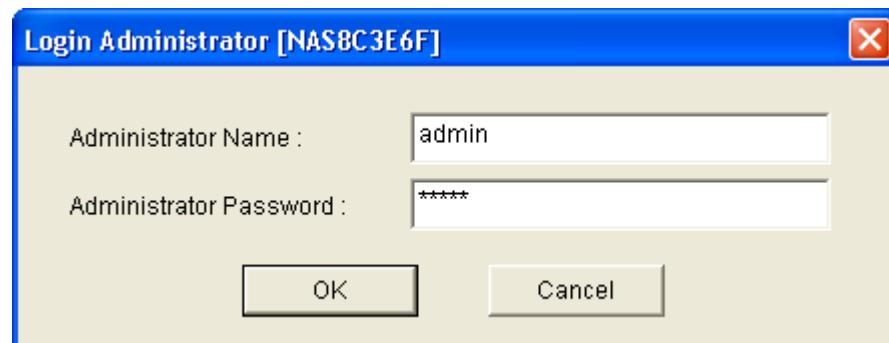
The system update may take tens of seconds to several minutes to complete depending on the network connection status. Please wait patiently. The system will inform you when system update is completed.

## **Update the system firmware by Finder**

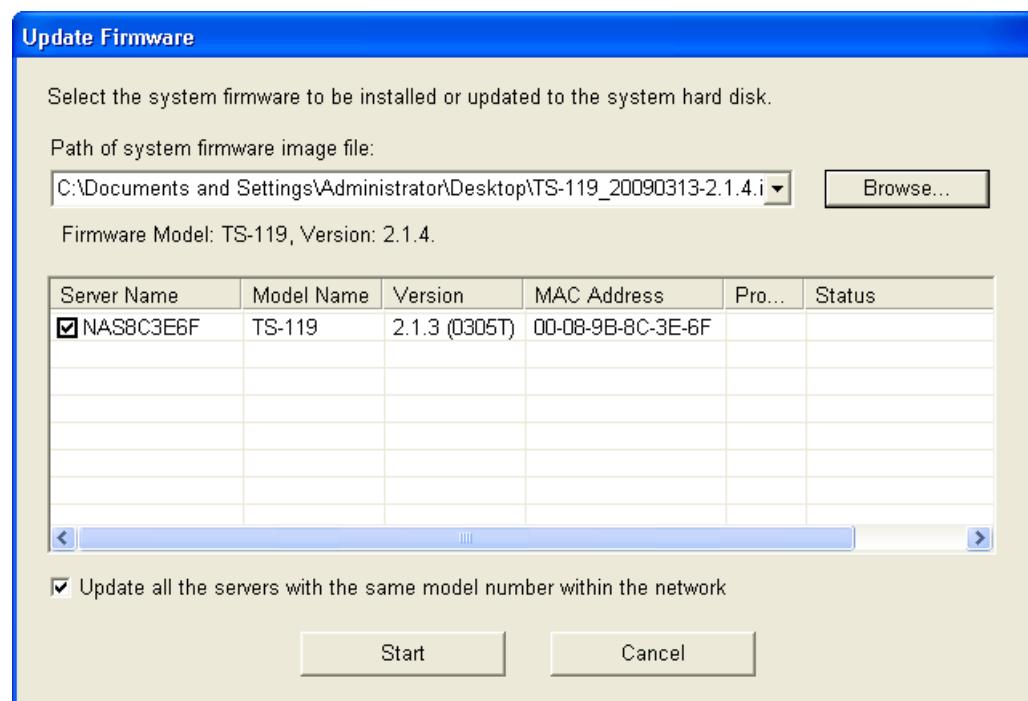
You can update the system firmware by QNAP Finder. Select a NAS model and click "Update Firmware" from the Tools menu.



Login as the administrator.



Browse and select the firmware for the NAS. Click "Start" to update the system.

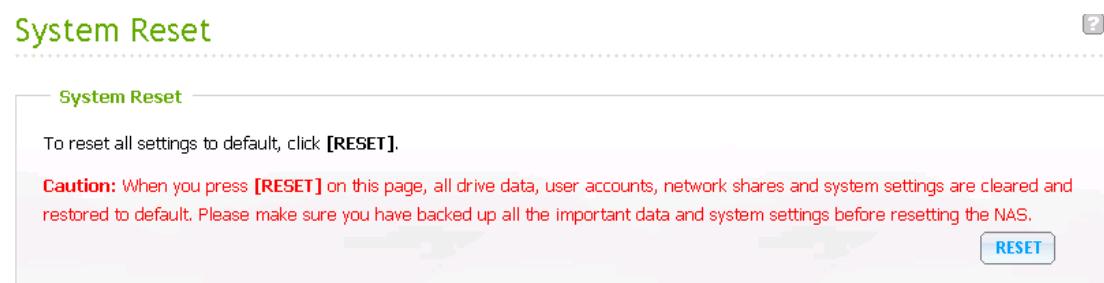


**Note:** You can use the Finder to update all the servers of the same model on the same local network. Make sure you have administrator access to all the servers you want to update.

### 3.1.11 System Reset

To reset all settings to default, click "RESET".

**Caution:** When you press "RESET" on this page, all the drive data, user accounts, network shares, and system settings are cleared and restored to default. Please make sure you have backed up all the important data and system settings before resetting the NAS.



## 3.2 Disk Management

The screenshot shows the 'Disk Management' section of a web-based interface. At the top, there's a navigation bar with 'Home >> Disk Management' on the left and 'Welcome admin | Logout English' on the right. Below the navigation bar, the title 'Disk Management' is displayed in green. There are six management options arranged in two rows of three:

- Volume Management**: Represented by an icon of three stacked hard drives.
- RAID Management**: Represented by an icon of two drives connected by a line.
- HDD SMART**: Represented by an icon of a drive with a magnifying glass over it.
- Encrypted File System**: Represented by an icon of a drive with a lock.

- iSCSI Target**: Represented by an icon of a cylinder labeled 'iSCSI Target' with '25%' and '75%'.
- Virtual Disk**: Represented by an icon of a stack of drives.

### 3.2.1 Volume Management

This page shows the model, size, and current status of the disk on the NAS. You can format and check disk, and scan bad blocks on the disk. When the disk is formatted, the NAS will create the following default share folders:

- ✓ Public: Network share for file sharing
- ✓ Qdownload: Network share for Download Station
- ✓ Qmultimedia: Network share for Multimedia Station
- ✓ Qusb: Network share for data copy function via USB ports
- ✓ Qweb: Network share for Web Server
- ✓ Qrecordings: the default network share of Surveillance Station

## Volume Management



Current Disk Volume Configuration: Physical Disks						
Disk	Model	Capacity	Status	Bad Blocks Scan	SMART Information	
Drive 1	Hitachi HDS721010KLA330 GKAO	931.51 GB	Ready	<a href="#">SCAN NOW</a>	<span style="color: green;">GOOD</span>	
Drive 2	--	--	No Disk	<a href="#">SCAN NOW</a>	---	
Drive 3	Seagate ST3160812AS 2AAA	149.05 GB	Ready	<a href="#">SCAN NOW</a>	<span style="color: green;">GOOD</span>	
Drive 4	Hitachi HDS721010KLA330 GKAO	931.51 GB	Ready	<a href="#">SCAN NOW</a>	<span style="color: green;">GOOD</span>	
Drive 5	--	--	No Disk	<a href="#">SCAN NOW</a>	---	

Current Disk Volume Configuration: Logical Volumes				
Volume	File System	Total Size	Free Size	Status
Single Disk: Drive 1	EXT4	915.42 GB	915.23 GB	Ready

Disk Configuration	Applied NAS Models
Single disk volume	All models
RAID 1, JBOD (just a bunch of disks)	2-bay models or above
RAID 5, RAID 6, RAID 5+hot spare,	4-bay models or above
RAID 6+hot spare	5-bay models or above

### ● Single Disk Volume

Each disk will be used as a standalone disk. However, if a disk is damaged, all data will be lost.

### ● RAID 1 Mirroring Disk Volume

RAID 1 (mirroring disk) protects your data by automatically backing up the contents of one drive onto the second drive of a mirrored pair. This protects your data if one of the drives fails. Unfortunately, the storing capacity is equal to a single drive, as the second drive is used to automatically back up the first.

Mirroring Disk is suitable for personal or corporate use to store important data.

### ● RAID 0 Striping Disk Volume

RAID 0 (striping disk) combines 2 or more drives into one larger disk. It offers the fastest disk access but it does not have any protection of your data if the

striped array fails. The disk capacity equals the number of drives in the array times the size of the smallest drive. Striping disk is usually used to maximize your disk capacity or for fast disk access but not for storing important data.

- **Linear Disk Volume (JBOD)**

You can combine two or more disks into one larger disk. During file saving, the file will be saved on physical disks sequentially but does not have a disk failure file protection function. The overall capacity of linear disk is the sum of all disks. Linear disk is generally used for storing large data and is not appropriate to use for file protection of sensitive data.

- **RAID 5 Disk Volume**

RAID 5 disk volume is ideal for organizations running databases and other transaction-based applications that require storage efficiency and data protection.

To create a RAID 5 disk volume, a minimum of 3 hard disks are required. The total capacity of RAID 5 disk volume = the size of the smallest capacity disk in the array x (no. of hard disk – 1). It's recommended that you use the same brand and same capacity hard drive to establish the most efficient hard drive capacity.

Additionally, if your system contains four disk drives, three of them can be used to implement RAID 5 data disks and the fourth drive can be used as a spare disk.

When a physical disk failure occurs, the system will automatically rebuild the data with the spare disk.

RAID 5 can survive 1 disk failure and system can still operate properly. When a disk fails in RAID 5, the disk volume will be in "degraded mode". There is no more data protection at this stage. If one more disk fails, all the data will be crashed. Therefore, you must replace a new disk immediately. You can install a new disk after turning off the server or hot swap the new disk when the server is on. The status of the disk volume will become "rebuilding" after installing a new disk. When rebuilding completes, your disk volume resumes to normal status.

**Note:** To install a disk when the server is on, make sure the disk volume is in "degraded" mode. Or wait for two long beeps after the disk crash, then insert the new disk.

- **RAID 6 Disk Volume**

RAID 6 disk volume is ideal for important data protection.

To create a RAID 6 disk volume, a minimum of 4 hard disks are required. The total capacity of RAID 6 disk volume = the size of the smallest capacity disk in the array x (no. of hard disk-2). It's recommended that you use same brand and same capacity hard drive to establish the most efficient hard drive capacity. RAID 6 can survive 2 drives failure and system can still operate properly.

**Note:** To install a disk when the server is on, make sure the disk volume is in "degraded" mode. Or wait for two long beeps after the disk crash, and then insert the new disk.

- **RAID 5, RAID 6 Read-only Mode**

The drive configuration enters read-only mode in the following occasions:

- 2 drives are damaged in RAID 5
- 3 drives are damaged in RAID 6

The drives in the above configurations are read-only. It is recommended to re-create new drive configuration in such case.

### 3.2.2 RAID Management

\* This function does not apply to one-bay model.

You can perform RAID capacity expansion, RAID level migration, or configure spare drive (RAID 5 only) with the data retained on this page.

Bitmap improves the time for RAID rebuilding after a crash, or removing or re-adding a member drive of the RAID configuration. If an array has a bitmap, the member drive can be removed and re-added and only blocks changes since the removal (as recorded in the bitmap) will be re-synchronized.

**Note:** Bitmap support is only available for RAID 1, 5, and 6.

**Recover:** When the NAS is configured as RAID 5 (or RAID 6) and 2 (or 3) hard drives are unplugged from the server accidentally, you can plug in the same hard drives into the same drive slots and click "Recover" to recover the volume status from "Not active" to "Degraded mode".

If the disk volume is configured as RAID 0 or JBOD and one or more of the drive members are disconnected, you can use this function to recover the volume status from "Not active" to "normal". The disk volume can be used normally after successful recovery.

**Note:** If the disconnected drive member is damaged, the RAID recovery function will not work.

#### RAID Management



This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved.

**Note:** Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Current Disk Volume Configuration				
Volume	Total Size	Bitmap	Status	Description
Single Disk: Drive 1	915.42 GB	--	Ready	The operation(s) you can execute: - Migrate
Single Disk: Drive 3	145.24 GB	--	Ready	The operation(s) you can execute: - Migrate
Single Disk: Drive 4	--	--	Unmounted	No operation can be executed for this drive configuration.

**Buttons:** EXPAND CAPACITY, ADD HARD DRIVE, MIGRATE, CONFIGURE SPARE DRIVE, BITMAP, RECOVER

For detailed instructions, please [click here](#).

For the online tutorial, please visit [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

### 3.2.3 HDD SMART

This page enables users to monitor hard drive health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.

Select the hard drive and you can view the following information by clicking the corresponding buttons.

Field	Description
Summary	Displays the hard drive smart summary and the latest test result.
Hard disk information	Displays the hard drive details, e.g., model, serial number, drive capacity, etc.
SMART information	Displays the hard drive SMART. Any items that the values are lower than the threshold are regarded as abnormal.
Test	To perform quick or complete hard drive SMART test and display the results.
Settings	To configure temperature alarm. When the hard drive temperature is over the preset values, the system records error logs. You can also configure quick and complete test schedule. The latest test result is shown in the Summary page.

**HDD SMART** 

Monitor hard disk health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.

Select hard disk  

**Summary**

**Good**

No errors were detected on the hard disk. Your hard disk should be operating properly.

<b>Hard disk model</b>	Western Digital Caviar Green family
<b>Drive capacity</b>	465.76 GB
<b>Hard drive health</b>	Good
<b>Hard drive temperature</b>	38 °C <input type="button" value=""/>
<b>Test time</b>	---
<b>Test result</b>	Not tested

### **3.2.4 Encrypted File System**

You can manage the encrypted disk volumes on the NAS on this page. Each encrypted disk volume is locked by a particular key. The encrypted volume can be unlocked by the following methods:

- Encryption Password: Enter the encryption password to unlock the disk volume. The default password is "admin".
- Encryption Key File: You can upload the encryption file to the server to unlock the disk volume. The key can be downloaded from "Encryption Key Management" page after you have unlocked the disk volume successfully.

#### **Encryption Key Management**

Volume	Total Size	Status	Action
Single Disk: Drive 1	915.42 GB	Unlocked	<b>ENCRYPTION KEY MANAGEMENT</b>
Single Disk: Drive 3	145.24 GB	Unlocked	<b>ENCRYPTION KEY MANAGEMENT</b>
Single Disk: Drive 4	--	Locked	<b>Input Encryption Password</b> <input type="password"/> <b>Open</b>

### 3.2.5 iSCSI

The NAS supports built-in iSCSI service. To use this function, follow the steps below:

1. Install an iSCSI initiator on your computer (Windows PC, Mac, or Linux).
2. Enable iSCSI Target Service on the NAS and create a new iSCSI target.
3. Run the iSCSI initiator and connect to the iSCSI target (NAS).
4. After successful logon, format the iSCSI target (disk volume). You can start to use the disk volume on the NAS as a virtual drive on your computer.

**Note:** The NAS supports 8 iSCSI devices at maximum.

For the online tutorial, please refer to [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

iSCSI Target Name	Capacity	Status	Action
iqn.2004-04.com.qnap:TS-509:iSCSI.test.B927B1	1.00 GB	Offline	

### 3.2.6 Virtual Disk

You can use this function to add the iSCSI targets of other QNAP NAS or storage servers to the NAS as the virtual disks for storage capacity expansion.

#### Virtual Disk

<input type="checkbox"/>	Name	File System	Total Size	Free Size	Status	Action
No virtual disk available.						
	<input type="button" value="Delete"/>					<input type="button" value="Add Virtual Disk"/>

To add a virtual disk to the NAS, make sure an iSCSI target has been created. Click "Add Virtual Disk".

<input type="checkbox"/>	Name	File System	Total Size	Free Size	Status	Action
No virtual disk available.						
	<input type="button" value="Delete"/>					<input type="button" value="Add Virtual Disk"/>

Enter the target server IP and port number (default: 3260). Click "Get Remote Disk". If authentication is required, enter the user name and password. Then, click "Apply".



Click to format the virtual disk.

Add Virtual Disk						
<input type="checkbox"/>	Name	File System	Total Size	Free Size	Status	Action
<input type="checkbox"/>	VirtualDisk1	Unknown	5 GB	0 MB	Unmounted	

When the status of the virtual disk is "Ready", you can start to use the virtual disk as a disk volume of the NAS. The NAS supports maximum 8 virtual disks.

### 3.3 Access Right Management

The files on the NAS can be shared among multiple users. For easier management and better control of users' access right, you have to organize users, user groups and their access right control.

The screenshot shows a web-based interface titled "Access Right Management". At the top, there is a navigation bar with "Home >> Access Right Management" on the left and "Welcome" on the right. Below the title, there are four main categories represented by icons: "Users" (green person icon), "User Groups" (blue group icon), "Share Folders" (yellow folder icon), and "Quota" (blue and red pie chart icon). Each category has its name written below its respective icon.

#### 3.3.1 Users

The system has created the following users by default:

- **admin**

By default, the administrator "admin" has access to system administration and cannot be deleted.

- **guest**

This is a built-in user and will not be displayed on User Management page. A guest does not belong to any user group. The login password for guest is guest.

- **anonymous**

This is a built-in user and will not be displayed on User Management page. When you connect to the server by FTP service, you can use this name to login as a guest.

**2048 users can be created at maximum** (including system default users). You can create a new user according to your needs. The following information is required to create a new user:

✓ **User name**

The user name must not exceed 32 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean except:

" / \ [ ] : ; | = , + \* ? < > ` '

✓ **Password**

The password is case-sensitive and can be 16 characters long at maximum. It is recommended to use a password of at least 6 characters.

Users			
Local Users		Actions	
	User Name	Quota	Action
<input type="checkbox"/>	admin	--	
	Delete	Total: 1   Display	10 entries per page.
			1 / 1

### 3.3.2 User Group

User group is a collection of users with the same access right to files or folders. The NAS has created the following user groups by default:

- **administrators**

All members in this group have administration right. You cannot delete this group.

- **everyone**

All registered users belong to everyone group. You cannot delete this group.

**256 groups can be created at maximum.** A group name must not exceed 256 characters. It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean, except the following ones:

" / \ [ ] : ; | = , + \* ? < > ` '

User Groups		
Local Groups		Create a User Group
	Group Name	Action
<input type="checkbox"/>	administrators	
<input type="checkbox"/>	everyone	

### 3.3.3 Share Folder

The primary purpose of network storage is file sharing. You can create different network share folders for various types of files, and provide different file access rights to users or user groups.

256 network shares can be created at maximum.

#### Share Folders

The screenshot shows a software interface titled "Share Folders". At the top right are two buttons: "New Share Folder" and "Restore default network shares". Below is a table with the following data:

	Folder Name	Size	Folders	Files	Hidden	Action
<input type="checkbox"/>	Network Recycle Bin 1	4 KB	0	0	No	
<input type="checkbox"/>	Public	56 MB	33	538	No	
<input type="checkbox"/>	Qdownload	8 KB	3	1	No	
<input type="checkbox"/>	Qmultimedia	90 MB	23	114	No	
<input type="checkbox"/>	Qrecordings	451 GB	1209	13773	No	
<input type="checkbox"/>	Qusb	4 KB	0	0	No	
<input type="checkbox"/>	Qweb	28 MB	801	5685	No	

At the bottom left are buttons for "Delete" and "Total: 7". A dropdown menu shows "Display 10 entries per page." On the right are navigation buttons for the table.

### 3.3.4 Quota

To allocate disk volume efficiently, you can specify the quota that can be used by each user. When this function is enabled and a user has reached his/her disk quota, he/she cannot upload data to the server anymore. By default, no limitations are set for users. You can modify the following two options:

- ✓ Enable quota for all users
- ✓ Quota size on each disk volume

**Quota** ?

---

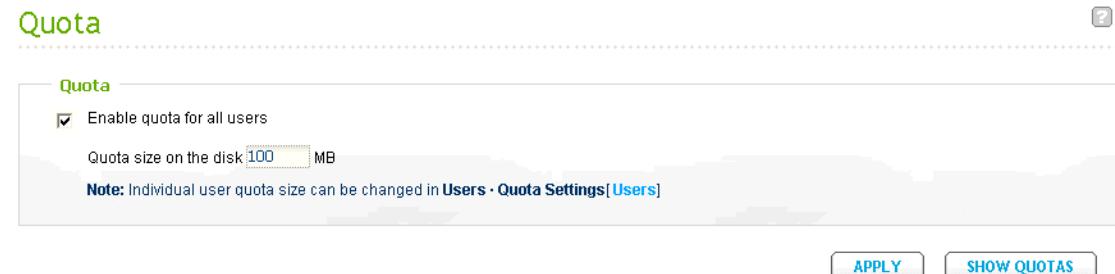
**Quota**

Enable quota for all users

Quota size on the disk:  MB

**Note:** Individual user quota size can be changed in [Users · Quota Settings](#) [[Users](#)]

[APPLY](#) [SHOW QUOTAS](#)



## 3.4 Network Services



### 3.4.1 Microsoft Networking

#### Microsoft Networking

**Microsoft Networking**

Enable file service for Microsoft networking

Standalone Server

AD Domain Member

Server Description:

Workgroup:

AD Server Name:

Domain Name:

Domain Username:

Password:

Enable WINS server

Use the specified WINS server

WINS server IP address:  .  .  .

Domain Master

**APPLY**

**Enable file service for Microsoft networking:** If you are using Microsoft® Windows®, enable this service to access the files on network share folders. Assign a workgroup name.

✓ **Standalone Server**

Use local users for user authentication.

✓ **AD Domain Member**

The NAS supports Windows 2003 AD (Active Directory) to provide quick and direct import of user accounts to the existing AD server available in your network. This function helps you to save time and effort on creating user accounts and passwords and lowers IT maintenance cost by automatic configuration procedure.

➤ **Server Description**

Describe the NAS for users to identify the server. To use the NAS on the Microsoft Windows OS, you must enable Microsoft Network Services.

➤ **Workgroup**

Specify the workgroup the NAS belongs to. The workgroup is a computer group unit in Microsoft Windows network for network sharing.

➤ **AD Server Name**

Enter the name of the AD server when AD domain is selected for authentication.

➤ **Domain Name**

The name of Microsoft domain. When you select AD domain, you must enter the domain name, the login user name, and the password.

✓ **WINS server**

If the local network has a WINS server installed, specify the IP address. The NAS will automatically register its name and IP address with WINS service. If you have a WINS server in your network and want to use this server, enter the WINS server IP.

✓ **Domain Master**

There is a unique Domain Master Browser for collecting and recording resources and services available for each PC in the network or workgroup of Windows. When you find the waiting time for accessing Network Neighborhood too long, it may be caused by failure of an existing master browser, or there is no master browser in the network. If there is no master browser in your network, you can check the box Domain Master in this section to configure the NAS as the master browser to enhance the speed of accessing information on Network Neighborhood.

### 3.4.2 Apple Networking

To access the NAS from Mac, enable AppleTalk Apple Filing Protocol network support.

If your AppleTalk network uses extended networks, and is assigned with multiple zones, assign a zone name to the NAS. If you do not want to assign a network zone, enter an asterisk (\*) to use the default setting. This setting is disabled by default.

**Apple Networking**

Apple Networking

Enable Apple Filing Protocol

Zone: \*

APPLY

### 3.4.3 NFS Service

To access the NAS from Linux, enable NFS service. For the information of connecting to the NAS via NFS on Linux, please refer to Chapter 11.

**NFS Service**

NFS Service

Enable NFS Service

You can set the allowed domain name and the access authority in Share Folder Management.  
[Click here to set the NFS access right of the network share.](#)

APPLY

### 3.4.4 FTP Service

When you enable FTP service, you can define the port number for the service and maximum number of users connected to the FTP at the same time.

#### FTP Service

**General**

Enable FTP Service

Protocol Type:  FTP (standard)  FTP with SSL/TLS (Explicit)

Port Number:

Unicode Support:  Yes  No

Enable Anonymous:  Yes  No

**Note:** If your FTP client does not support Unicode, please select "No" for Unicode Support and select a supported filename encoding from [\[Filename Encoding\]](#) under [System Settings] so that the folders and files on FTP can be properly shown.

**Connection**

Maximum Number of all FTP connections:

Maximum Number of Connections For a Single Account:

Enable FTP transfer limitation

Maximum upload rate (KB/s):  KB/s

Maximum download rate (KB/s):  KB/s

**Advanced**

Passive FTP Port Range:  Use the default port range(55536 - 56559)  Define port range:  -

✓ **Select Protocol Type**

Select to use standard FTP connection or SSL/TLS encrypted FTP. Select the corresponding protocol type in your client FTP software to ensure successful connection.

✓ **Unicode Support**

Select to enable or disable Unicode Support. The default setting is No. Since most FTP clients do not support Unicode currently, it is recommended that you disable Unicode support here and select the language the same as your OS in "General Settings" > "Language" page so that the folders and files on FTP can be properly shown. If your FTP client supports Unicode, make sure you have enabled Unicode support for both your client and the NAS.

✓ **Anonymous Login**

You can enable anonymous login to allow users to access the FTP server of the NAS anonymously. The users can access the folders and files which are opened for public access. If this option is disabled, users must enter an authorized user name and password to access the server.

✓ **Passive FTP Port Range**

You can use the default port range (55536-56559) or define a port range larger than 1023. When using this function, please make sure you have opened the configured port range on your router or firewall.

✓ **FTP Transfer Limitation**

You can configure the maximum number of all FTP connections, maximum connections of a single account and the maximum upload/ download rates of a single connection.

✓ **Respond with external IP address for passive FTP connection request**

When passive FTP connection is in use and the FTP server is configured under a router, if the remote computer cannot connect to the FTP server via WAN, you can enable this function. By enabling this function, the FTP service replies the manually specified IP address or automatically detects the external IP address so that the remote computer can connect to the FTP server successfully.

### 3.4.5 Telnet/SSH

After enabling this option, you can access this server via Telnet or SSH encrypted connection (only the account “admin” can login remotely). You can use certain Telnet or SSH connection clients for connection, e.g. putty. Please make sure you have opened the configured ports on your router or firewall when using this function.

Telnet / SSH

---

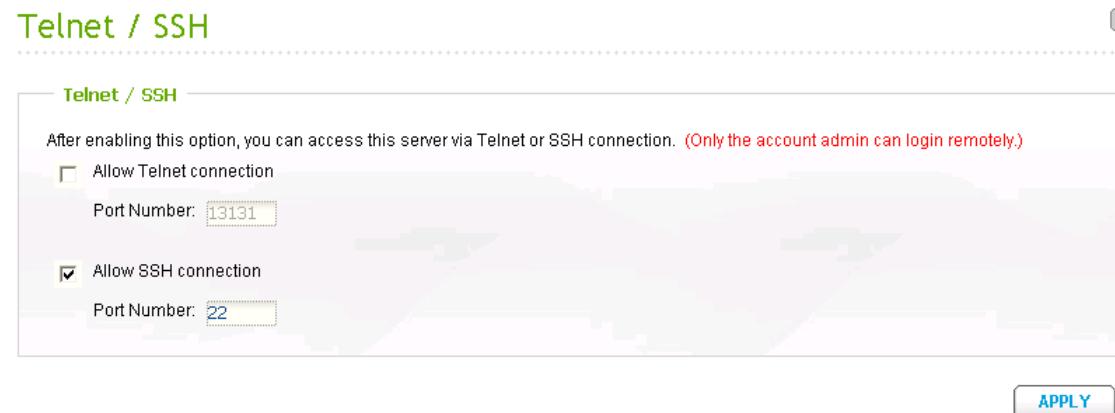
**Telnet / SSH**

After enabling this option, you can access this server via Telnet or SSH connection. (Only the account admin can login remotely.)

Allow Telnet connection  
Port Number:

Allow SSH connection  
Port Number:

**APPLY**



### **3.4.6 SNMP Settings**

You can enable SNMP (Simple Network Management Protocol) service on the NAS and enter the trap address of the SNMP management stations (SNMP manager), e.g. PC with SNMP software installed. When an event, warning, or error occurs on the NAS, the NAS (as an SNMP agent) reports the real-time alert to the SNMP management stations.

The fields are described as below:

<b>Field</b>	<b>Description</b>
Community	An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the NAS. The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Send Event	Select the type of events to be reported to the SNMP manager. You can find the detailed logs on the "System Logs" page.
Trap Address	The IP address of the SNMP manager. You can enter up to 3 trap addresses.
SNMP MIB (Management Information Base)	The MIB is a type of database in ASCII text format used to manage the NAS in the SNMP network. The SNMP manager uses the MIB to determine the values or understand the messages sent from the agent (NAS) within the network. You can download the MIB and view it with any word processor or text editor.

## SNMP Settings



### SNMP

After enabling this service, the NAS will be able to report information via SNMP to the managing systems.

Enable SNMP Service

Port Number:

Community:

Send Event:  Information  Warning  Error

Trap Address 1:

Trap Address 2:

Trap Address 3:

**APPLY**

### SNMP MIB

To install the MIB to your managing systems, click **[Download]**.

**DOWNLOAD**

### 3.4.7 Web Server

You can publish your own server by enabling Web Server function of the NAS. Enter the port number for web server service, the default number is 80. For further information, please refer to Chapter 6.

Web Server

Web Server

After enabling this function, you can upload the webpage files to "Qweb" network share to publish your website.

Enable Web Server

Port Number:

register\_globals:  On  Off

After enabling this service, click the following link to enter to Web Server.  
<http://10.8.10.19:80/>

APPLY

php.ini Maintenance

php.ini Maintenance

The file **php.ini** is the system configuration file of Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended to use the system default setting.

#### Configure register\_globals

Select to enable or disable register\_globals. The setting is disabled by default. When the web program asks to enable php register\_globals, please enable this option. However, for system security concerns, it is recommended to disable this option.

#### php.ini Maintenance

Check the box "php.ini Maintenance" to select to upload, edit or restore php.ini.

- Edit: Edit the current php.ini file.
- Upload: Upload a new php.ini file to replace the current file.
- Restore: Restore the php.ini file to system default.

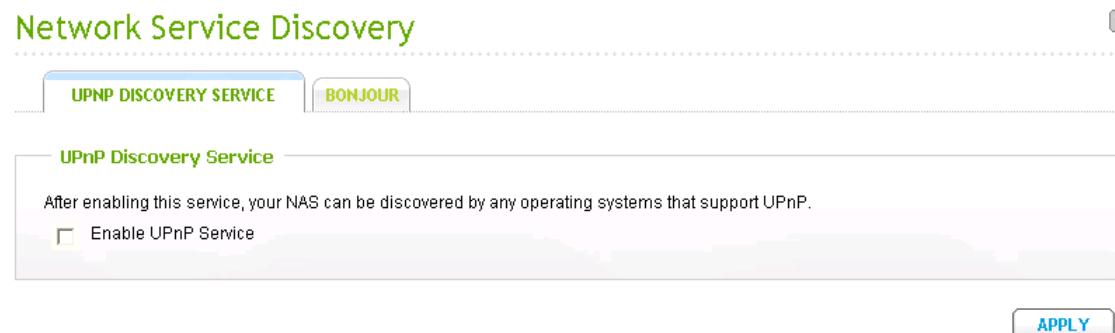
**Note:** To use PHP mail() function, you can go to "System Administration" > "Notification" > "Configure SMTP Server" to configure the SMTP server settings.

## 3.4.8 Network Service Discovery

### 3.4.8.1 UPnP Discovery Service

When a device is added to the network, the UPnP discovery protocol allows the device to advertise its services to the control points on the network.

By enabling the UPnP Discovery Service, the NAS can be discovered by any operating systems that support UPnP.



### 3.4.8.2 Bonjour

By broadcasting the network service(s) with Bonjour, your Mac will automatically discover the network services (e.g. FTP) which are running on the NAS without the need to enter the IP addresses or configure the DNS servers.

**Note:** You will have to activate each service (e.g. FTP) on its setup page, and then enable the service on the Bonjour page, so that the NAS will advertise this service with Bonjour.

Network Service Discovery

UPNP DISCOVERY SERVICE    BONJOUR

Bonjour

Before broadcasting the following services through Bonjour, please DO NOT forget to enable these services first.

Web Administration  
Service Name KENTS219

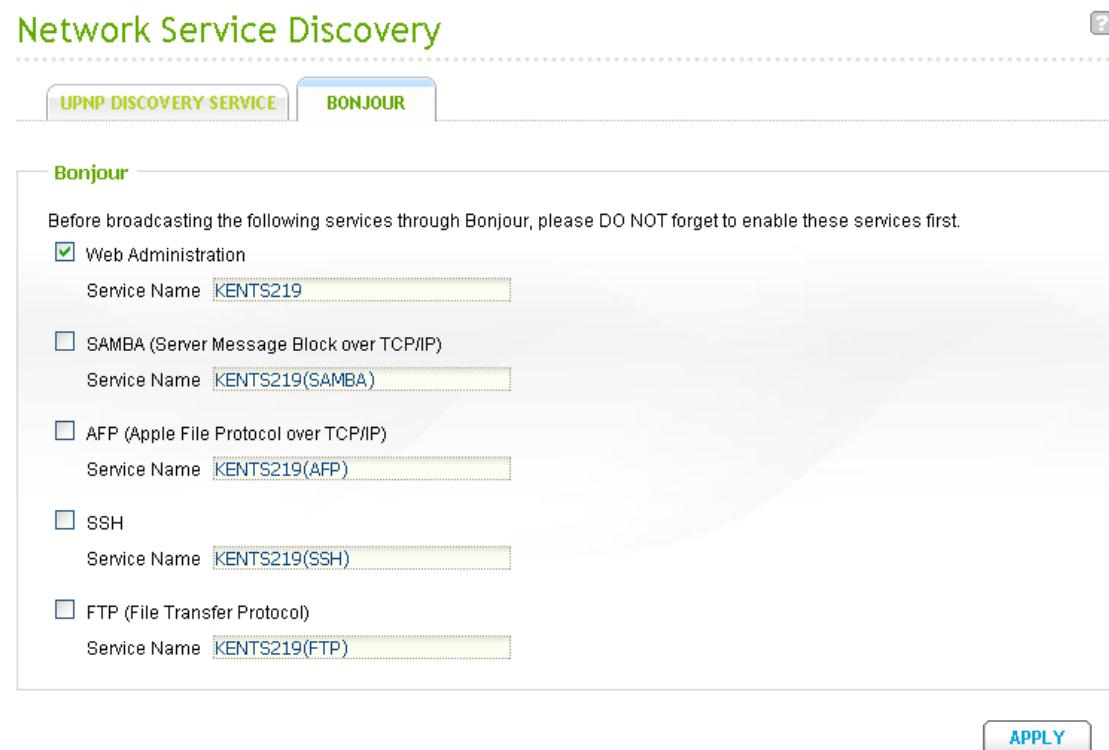
SAMBA (Server Message Block over TCP/IP)  
Service Name KENTS219(SAMBA)

AFP (Apple File Protocol over TCP/IP)  
Service Name KENTS219(APP)

SSH  
Service Name KENTS219(SSH)

FTP (File Transfer Protocol)  
Service Name KENTS219(FTP)

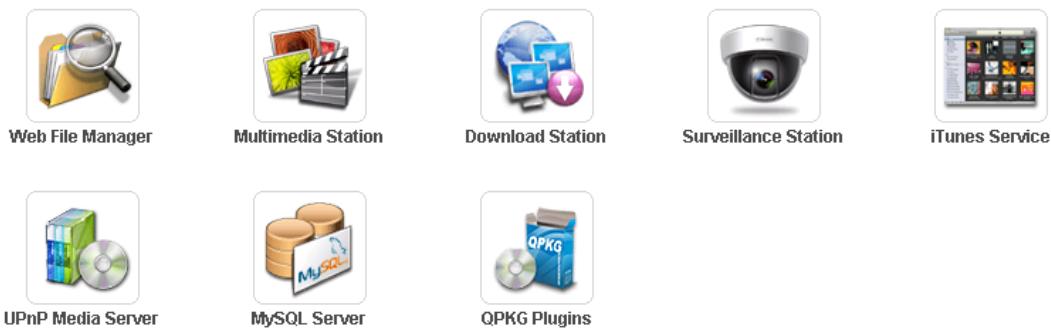
APPLY



## 3.5 Applications

Home >> Applications      Welcome admin | Logout      English

### Applications



### 3.5.1 Web File Manager

To access the NAS via the web browser, enable Web File Manager. If the NAS is connected to the Internet and uses a valid IP address, you can access files on the server by web browser from anywhere. For more information, please refer to Chapter 8.

#### Web File Manager

<input checked="" type="checkbox"/> Web File Manager
<input checked="" type="checkbox"/> Enable Web File Manager
<input type="button" value="APPLY"/>

### 3.5.2 Multimedia Station

To share photos, music or video files on the NAS over the network, enable Multimedia Station. For further information of Multimedia Station, iTunes service and UPnP Media Server, please refer to Chapter 4.

#### Multimedia Station

Multimedia Station

Enable Multimedia Station  
 Show service link on the login page.

APPLY

### 3.5.3 Download Station

The NAS supports PC-less BT, HTTP, and FTP download. To use download function of the NAS, please enable Download Station. For further information, please refer to Chapter 5.

#### Download Station

Download Station

Enable Download Station  
 Show service link on the login page.

APPLY



**Warning:** Please be warned against illegal downloading of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions of the copyright laws and should accept all the consequences.

### 3.5.4 Surveillance Station

The Surveillance Station enables you to monitor and record the live video of maximum 2-4\* network cameras available on the network (LAN or WAN).

\*This function is applicable to some models only. Please refer to the comparison table for more details:

[http://www.qnap.com/images/products/comparison/Comparison\\_NAS.html](http://www.qnap.com/images/products/comparison/Comparison_NAS.html)

**Note:** To use this feature on TS-x39/509/809 series, please update the system firmware with the image file enclosed in the product CD or download the latest system firmware.

The screenshot shows a configuration panel for the Surveillance Station. It includes two checked checkboxes: "Enable Surveillance Station" and "Show service link on the login page". Below the checkboxes is a blue "APPLY" button.

Click "Surveillance Station" on the top or on the login page of NAS to access the Surveillance Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.



**Note:** The Surveillance Station is only supported on IE browser 6.0 or later.

To set up your network surveillance system by NAS, follow the steps below:

1. Plan your home network topology
2. Set up the IP Cameras
3. Configure the camera settings on NAS
4. Configure your NAT router (for remote monitoring over the Internet)

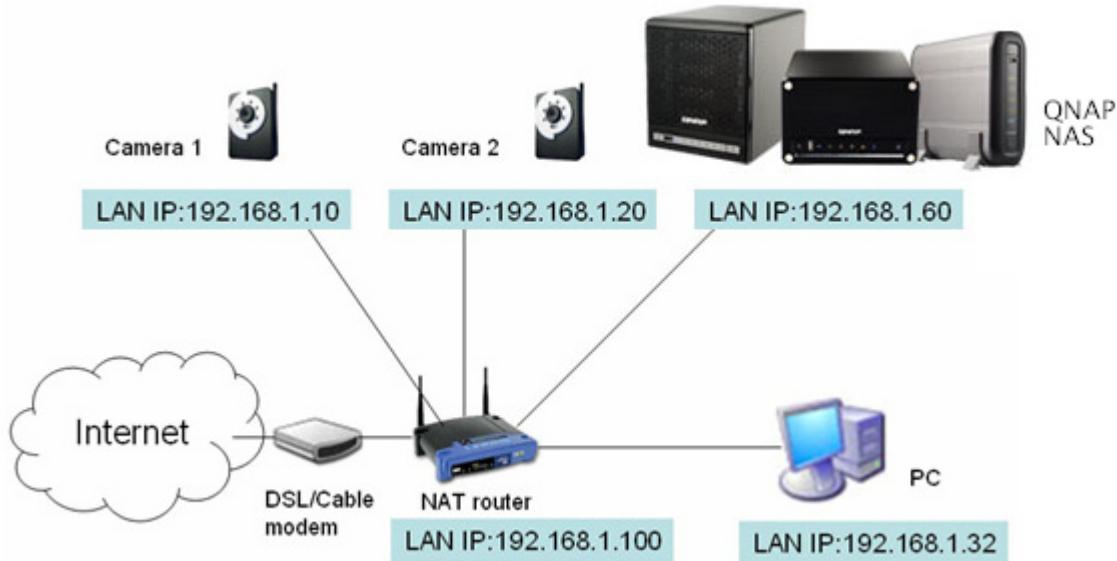
### **1. Plan your home network topology**

Write down your plan of the home network before starting to set up the surveillance system. Consider the following when doing so:

- i. The IP address of NAS
- ii. The IP address of the cameras

Your computer, the NAS, and the IP cameras should be installed to the same router in LAN. Assign fixed IP addresses to the NAS and the IP cameras. For example,

- The LAN IP of the home router: 192.168.1.100
- Camera 1 IP: 192.168.1.10 (fixed IP)
- Camera 2 IP: 192.168.1.20 (fixed IP)
- NAS IP: 192.168.1.60 (fixed IP)



## 2. Set up the IP Cameras

In this example, two IP cameras will be installed. Connect the IP cameras to your home network. Then set the IP address of the cameras so that they are in the same LAN as the computer. Login the configuration page of the Camera 1 by IE browser. Enter the IP address of the first camera as 192.168.1.10. The default gateway should be set as the LAN IP of the router (192.168.1.100 in this example). Then configure the IP address of the second camera as 192.168.1.20.

Some cameras provide a utility for IP configuration. You may refer to the user manual of the cameras for further details.

\* Please refer to [www.qnap.com](http://www.qnap.com) for the supported network camera list.

## 3. Configure the camera settings on NAS

Login the Surveillance Station by IE browser to configure the IP cameras. Go to "Settings>Camera Settings" page. Enter the camera information, e.g. name, model, and IP address.

The screenshot shows the QNAP Surveillance Station interface. At the top, there's a navigation bar with tabs: Home, Settings (which is selected), Live View, Playback, and Log. Below the navigation bar is a sub-menu with tabs: Camera Settings (selected), Recording Settings, Schedule Settings, and Advanced Settings. The main content area displays a table of cameras:

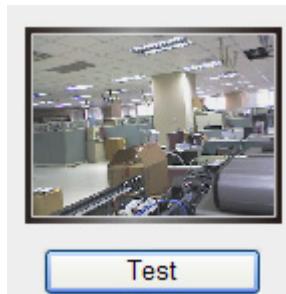
	Camera Name	Brand	IP Address	WAN IP Address
1	Camera 1			
2	Camera 2			

Below the table, there are configuration fields for Camera 1:

- Camera Number: 1: Camera 1
- Camera Model: Axis 205
- Camera Name: Camera 1
- IP Address: (input field)
- Port: 80
- WAN IP: (for monitoring from public network)  
(If your IP camera is installed behind NAT router, you may input the public IP address (or URL) and the corresponding forwarded port of the router.)  
Port: 80
- User Name: (input field)
- Password: (input field)

At the bottom of the form are two buttons: "Apply" and "Remove". A note at the bottom states: "Note: All the camera configuration will not take effect until you click the "Apply" button."

Click "Test" on the right to ensure the connection to the IP camera is successful.



If your camera supports audio recording, you may enable the option in "Recording Settings" page. Click "Apply" to save the changes.

Camera Number:	2: Camera 2
Video Compression:	Motion JPEG
Resolution:	QVGA
Frame Rate:	20
Quality:	Normal

Enable audio recording on this camera

Estimated Storage Space for Recording: 6760 GB

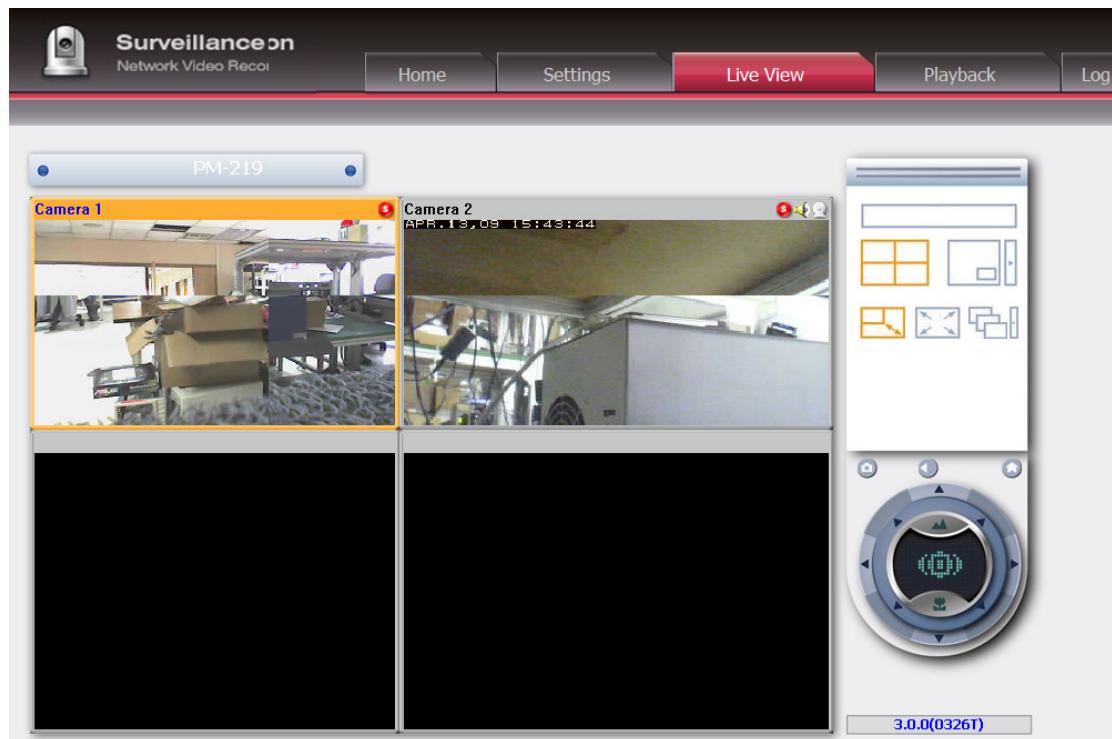
**Apply**

A configuration form for a network camera. It includes dropdown menus for Camera Number (set to 2: Camera 2), Video Compression (set to Motion JPEG), Resolution (set to QVGA), Frame Rate (set to 20), and Quality (set to Normal). There is also a checked checkbox for enabling audio recording. Below the form, a message indicates the estimated storage space for recording is 6760 GB, and at the bottom is a prominent blue "Apply" button.

Configure the settings of Camera 2 following the above steps.

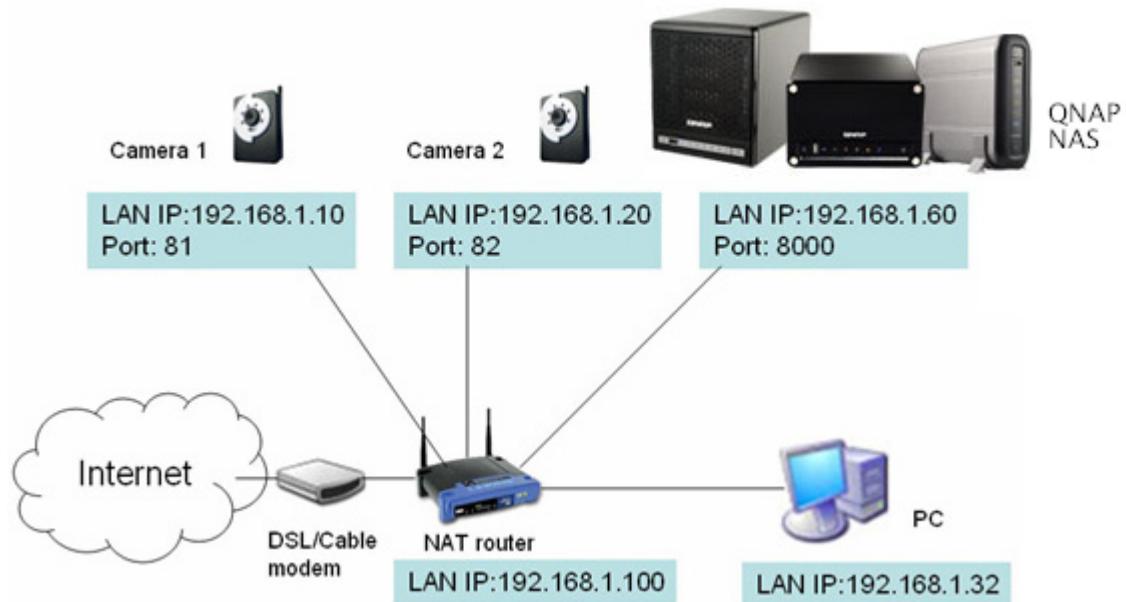
After you have added the network cameras to NAS, go to the "Live View" page. The first time you access this page by IE browser, you have to install the ActiveX control in order to view the images of Camera 1 and Camera 2. You can start to use the monitoring and recording functions of the Surveillance Station.

To use other functions of the Surveillance Station such as motion detection recording, schedule recording, and video playback, please refer to the online help.



#### 4. Configure your NAT router (for remote monitoring over the Internet)

To view the monitoring video and access the NAS remotely, you need to change the network settings by forwarding different ports to the corresponding LAN IP on your NAT router.



Change the port settings of NAS and IP cameras

The default HTTP port of NAS is 8080. In this example, the port is changed to 8000.

Therefore, you have to access the NAS via **http://NAS IP:8000** after applying the settings.

Then login the network settings page of the IP cameras. Change the HTTP port of Camera 1 from 80 to 81. Then change the port for Camera 2 from 80 to 82.

Next, login Surveillance Station. Go to "Settings>Camera Settings". Enter the port numbers of Camera 1 and Camera 2 as 192.168.1.10 **port 81** and 192.168.1.20 **port 82** respectively. Enter the login name and password for both cameras.

Besides, enter the WAN IP address (or your domain address in public network, e.g. MyNAS.dyndns.org) and the port on the WAN side for the connection from Internet. After finishing the settings, click "Test" to ensure successful connection to the cameras.

The screenshot shows the "Camera Settings" configuration interface. It includes fields for Camera Number (set to 1: Camera 1), Camera Model (iPUX ICS 1003/1013), Camera Name (Camera 1), IP Address (192.168.1.10), Port (81), WAN IP (myNAS.dyndns.org), User Name (administrator), and Password (\*\*\*\*\*). There are checkboxes for "Port" and "WAN IP" (disabled). A "Test" button is visible next to the WAN IP field. At the bottom, there are "Apply" and "Remove" buttons, and a note: "Note: All the camera configuration will not take effect until you click the "Apply" button."

Go to the configuration page of your router and configure the port forwarding as below:

- Forward Port 8000 to NAS LAN IP: 192.168.1.60
- Forward Port 81 to Camera 1's LAN IP: 192.168.1.10
- Forward Port 82 to Camera 2's LAN IP: 192.168.1.20

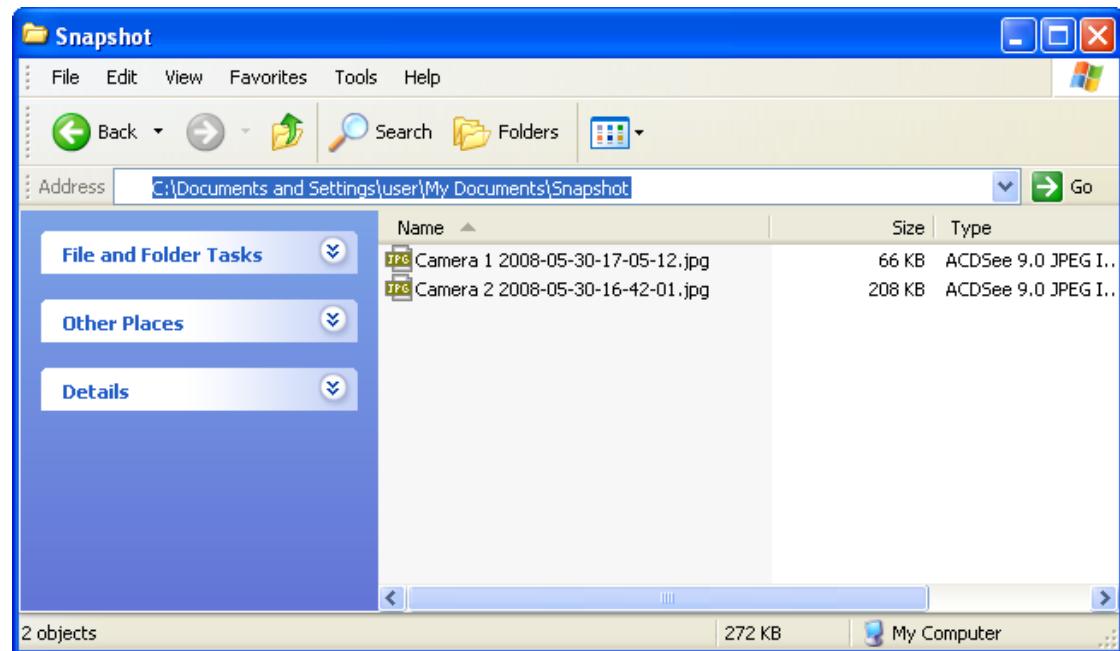
**Note:** When you change the port settings, make sure remote access is allowed.

For example, if you office network blocks port 8000, you will not be able to access your NAS from the office.

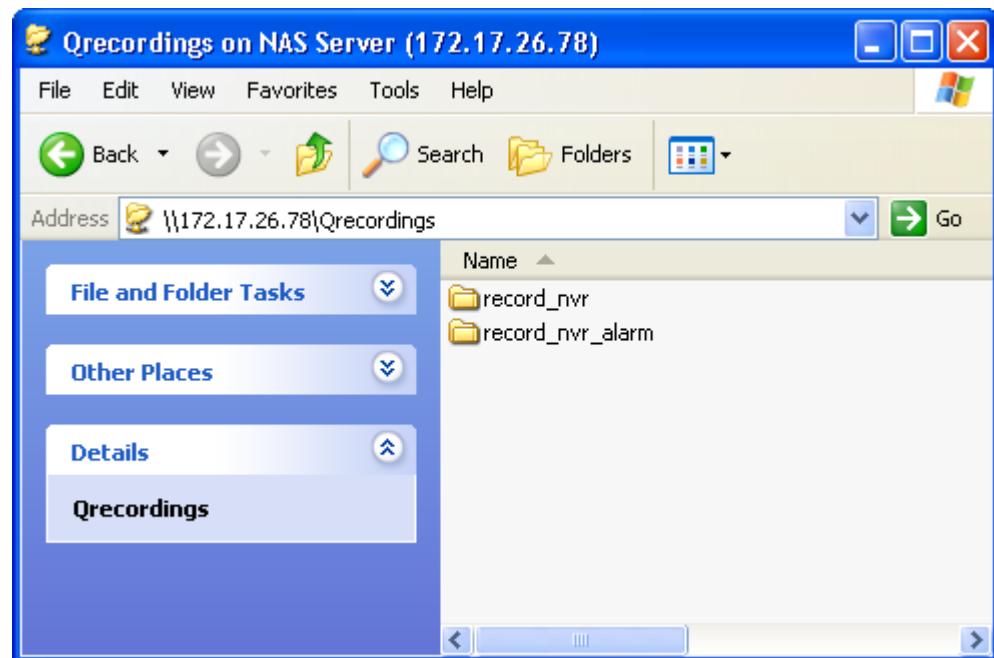
After you have configured the port forwarding and router settings, you can start to use the Surveillance Station for remote monitoring over the Internet.

## Access the snapshots and video recordings of Surveillance Station

All snapshots taken are saved in the "Snapshot" folder under My Documents in your computer.



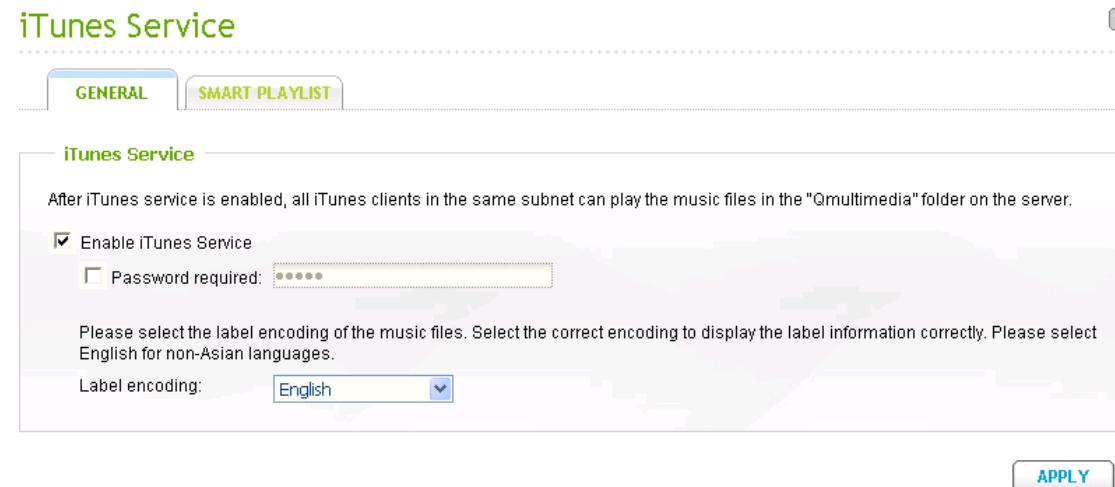
The video recordings will be saved in <\\NASIP\Qrecordings>. Normal recordings are saved in the folder "record\_nvr" and alarm recordings are saved in the folder "record\_nvr\_alarm" in the network share.



### 3.5.5 iTunes Service

The mp3 files on Qmultimedia folder of the NAS can be shared to iTunes by enabling this service. All the computers with iTunes installed on LAN are able to find, browse, and play the music files on the NAS.

To use the iTunes service, make sure you have installed the iTunes program on your computer. Enable this service. Then upload the music files to the Qmultimedia folder of NAS.



**Password required:** To allow the users to access the data only by entering the correct password, check this option and enter the password.

Click "Smart Playlist" to enter the smart playlist page. You can define the playlist rules to categorize the songs into different playlists. If there is no song that matches the rules in the playlist, the iTunes client will not show the playlist. For detailed operation, please refer to the online help.



When you open iTunes, it detects the NAS automatically. All the songs on the Qmultimedia folder will be shown.

Name	Time	Artist	Album	Genre	Rating
Winter Wonderland	2:59	Lisa Ono	Boas Festas	Jazz	
Depois Do Natal	2:58	Lisa Ono	Boas Festas	Jazz	
Let It Snow! Let It Snow! Let It S...	3:48	Lisa Ono	Boas Festas	Jazz	
Caroling Caroling	3:56	Lisa Ono	Boas Festas	Jazz	
Jingle Bell Rock	2:20	Lisa Ono	Boas Festas	Jazz	
White Christmas (Noite de Natal)	3:48	Lisa Ono	Boas Festas	Jazz	
Paz Azul (Brahms Lullaby)	3:39	Lisa Ono	Boas Festas	Jazz	
Ave Maria	3:56	Lisa Ono	Boas Festas	Jazz	
The Christmas Song	3:41	Lisa Ono	Boas Festas	Jazz	
Boas Festas	4:44	Lisa Ono	Boas Festas	Jazz	
Um Anjo Do Céu	5:28	Lisa Ono	Boas Festas	Jazz	
In the Wee Small Hours of the Mo...	4:37	Lisa Ono	Boas Festas	Jazz	
Silent Night	1:01	Lisa Ono	Boas Festas	Jazz	
01 Beautiful Woman.mp3	0:07			Color your soul	Other
02 Salesman.mp3	3:44				
03 Fill This Night.mp3	4:17				
04 Cry Out Loud.mp3	4:19				
05 I Will Give You Everything.mp3	4:00				
06 Come Alive.mp3	4:50				
07 날짜 번경선.mp3	3:45				
08 Be My Love (English Ver.), (Ho...	4:33				
09 품.mp3	4:43				
10 Color Your Soul.mp3	4:50				
11 Speechless.mp3	3:13				

The iTunes MiniStore helps you discover new music and video right from your iTunes Library. As you select tracks or videos in your Library, information about your selections are sent to Apple and the MiniStore will display related songs, artists, or videos. Apple does not keep any information related to the contents of your iTunes Library.

Would you like to turn on the MiniStore now? [Turn on MiniStore](#)

If you don't want to turn the MiniStore on now, click Not Now. You can always access this page again and turn the MiniStore on at any time by selecting Show MiniStore from the View menu.

[Not Now](#)

INSIDE THE STORE: Demon Days Gorillaz Released 2005 ★★★½  
Reviews Gift This Music Tell a Friend

MORE FROM GORILLAZ: Feel Good Inc. Gorillaz Released 2005 ★★★★½  
Reviews Gift This Music Tell a Friend

Gorillaz Gorillaz Released 2001 ★★★½  
Reviews Gift This Music Tell a Friend

Click the triangle icon next to the NAS name. The smart playlists defined earlier will be shown. The songs are categorized accordingly. You can start to use iTunes to play the music on your NAS.

The screenshot shows the iTunes interface. The menu bar includes File, Edit, Controls, View, Store, Advanced, and Help. The main window displays a library of songs. The left sidebar shows categories: LIBRARY (Music, Movies, TV Shows, Podcasts, Radio), STORE (iTunes Store), and SHARED (NASAC68C6, color your soul, Jazz, Lisa Ono). The right pane is a table listing 13 songs:

	Name	Time	Artist	Album	Genre
1	Winter Wonderland	2:59	Lisa Ono	Boas Festas	Jazz
2	Depois Do Natal	2:58	Lisa Ono	Boas Festas	Jazz
3	Let It Snow! Let It Snow! Let It S...	3:48	Lisa Ono	Boas Festas	Jazz
4	Caroling Caroling	3:56	Lisa Ono	Boas Festas	Jazz
5	Jingle Bell Rock	2:20	Lisa Ono	Boas Festas	Jazz
6	White Christmas (Noite de Natal)	3:48	Lisa Ono	Boas Festas	Jazz
7	Paz Azul (Brahms Lullaby)	3:39	Lisa Ono	Boas Festas	Jazz
8	Ave Maria	3:56	Lisa Ono	Boas Festas	Jazz
9	The Christmas Song	3:41	Lisa Ono	Boas Festas	Jazz
10	Boas Festas	4:44	Lisa Ono	Boas Festas	Jazz
11	Um Anjo Do Céu	5:28	Lisa Ono	Boas Festas	Jazz
12	In the Wee Small Hours of the Mo...	4:37	Lisa Ono	Boas Festas	Jazz
13	Silent Night	1:01	Lisa Ono	Boas Festas	Jazz

**Note:** You can download the latest iTunes software from official Apple website  
<http://www.apple.com>.

### 3.5.6 UPnP Media Server

The NAS is built-in with TwonkyMedia, DLNA compatible UPnP media server. Enable this function and the NAS will share particular music, photos, or video files to DLNA network. You can use DLNA compatible digital media player (DMP), to play the multimedia files on the NAS on TV or acoustic sound system.

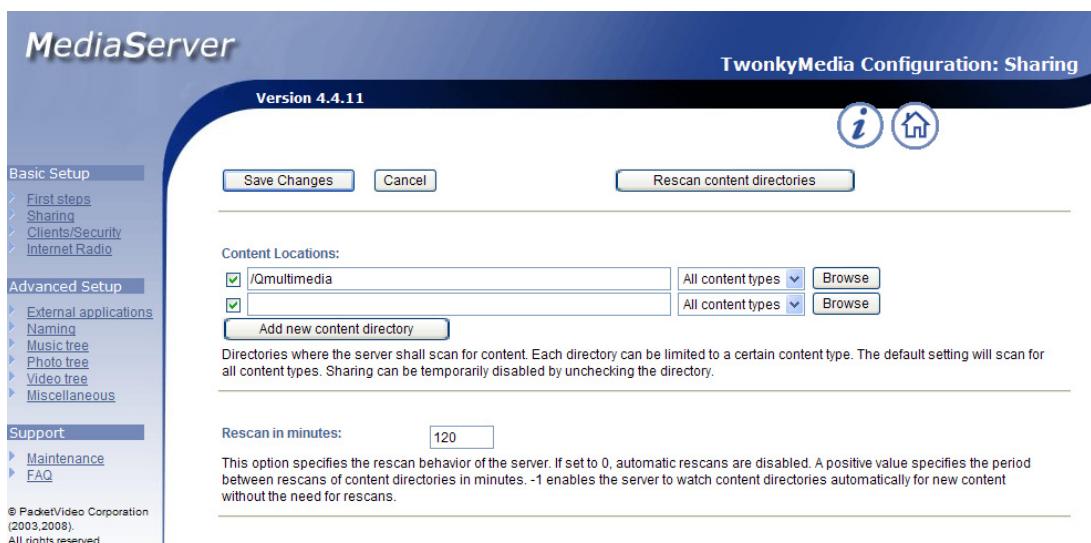
To use UPnP Media Server, please enable this function and click the following link (<http://NAS IP:9000/>) to enter the configuration page of UPnP Media Server.



Click the link <http://NAS IP:9000/> to enter UPnP Media Server configuration page and configure the following settings.

- (1) Language: Select the display language.
- (2) Server Name: Enter the name of NAS UPnP Media Server. This name will be shown on DMP operation interface, e.g. NAS.
- (3) Content Locations: Select the share folder on the NAS to be shared to DMP. The default folder is Qmultimedia. You can add more than one share folder.

Click "Save Changes" to save the settings.



After configuring the settings, you can upload mp3, photos, or video files to Qmultimedia folder or other specified folders on the NAS.

**Note:** If you upload multimedia files to the default share folder but the files are not shown on Media Player, you can click "Rescan content directories" or "Restart server" on the Media Server configuration page.

The built-in UPnP Media Server of the NAS is compatible with the DLNA DMP devices in the market.

For the online tutorial, please visit [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

### **About UPnP and DLNA**

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. The purpose of UPnP is to allow devices to connect seamlessly and to simplify the implementation of networks at home and in corporate environment. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.

The term UPnP is gleaned from Plug-and-play, a technology for dynamically attaching devices to a computer directly.

The Digital Living Network Alliance (DLNA) is an alliance of a number of consumer electronics, mobile and personal computer manufacturers. Its aim is to establish a home network in which the electronic devices from all companies are compatible with each other under an open standard. The alliance also tries to promote the idea of digital home by establishing DLNA certification standard. All DLNA certified products connected to the home network can be accessed seamlessly to enable consumers to enjoy digital life conveniently.

### 3.5.7 MySQL Server

#### MySQL Server

You can enable MySQL server as the website database.

Enable MySQL Server  
Enable this option to allow remote connection of MySQL server.

Enable TCP/IP Networking

Port Number:

**APPLY**

You can reset the database password or re-initialize the database.

**RESET ROOT PASSWORD** **RE-INITIALIZE DATABASE**

**Note:** To use this feature on TS-x39/509/809 series, please update the system firmware with the image file enclosed in the product CD or download the latest system firmware.

You can enable MySQL Server as the website database.

#### Enable TCP/IP Networking

You can enable this option to configure MySQL Server of the NAS as a database server of another web server in remote site through Internet connection. When you disable this option, your MySQL Server will only be configured as local database server for the web server of the NAS.

After enabling remote connection, please assign a port for the remote connection service of MySQL server. The default port is 3306.

After the first-time installation of the NAS, a folder phpMyAdmin is created in the Qweb network folder. You can enter <http://NAS IP/phpMyAdmin/> in the web browser to enter the phpMyAdmin page and manage the MySQL database.

**Note:**

- Please do not delete the phpMyAdmin folder. You can rename this folder but the link on the MySQL Server page will not be updated. To access the renamed folder, you can enter the link <http://NAS IP/renamed folder> in the web browser.
- The phpMyAdmin folder is created after the first-time installation. When you update the firmware, the folder remains unchanged.

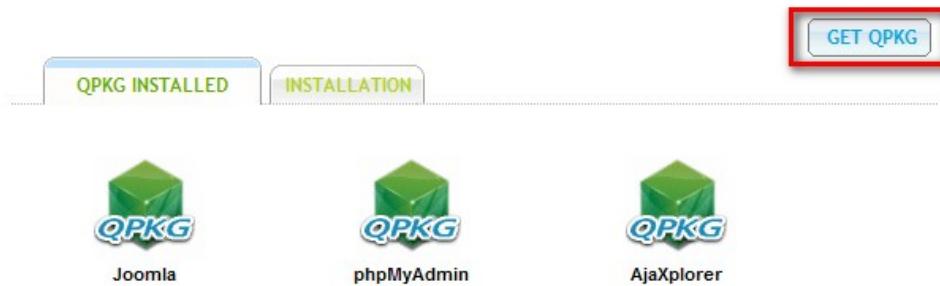
### **Database Maintenance**

- Reset root password: Execute this function to reset the password of MySQL root as “**admin**”.
- Re-initialize database: Execute this function to delete all the data on MySQL database.

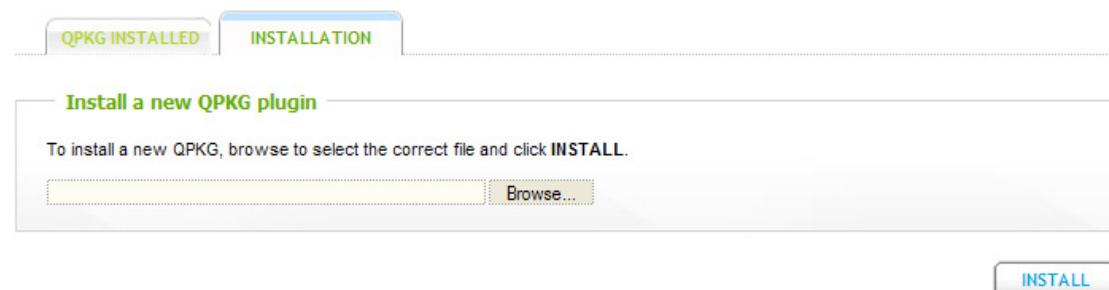
For the online tutorial, please refer to [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

### 3.5.8 QPKG Plugins

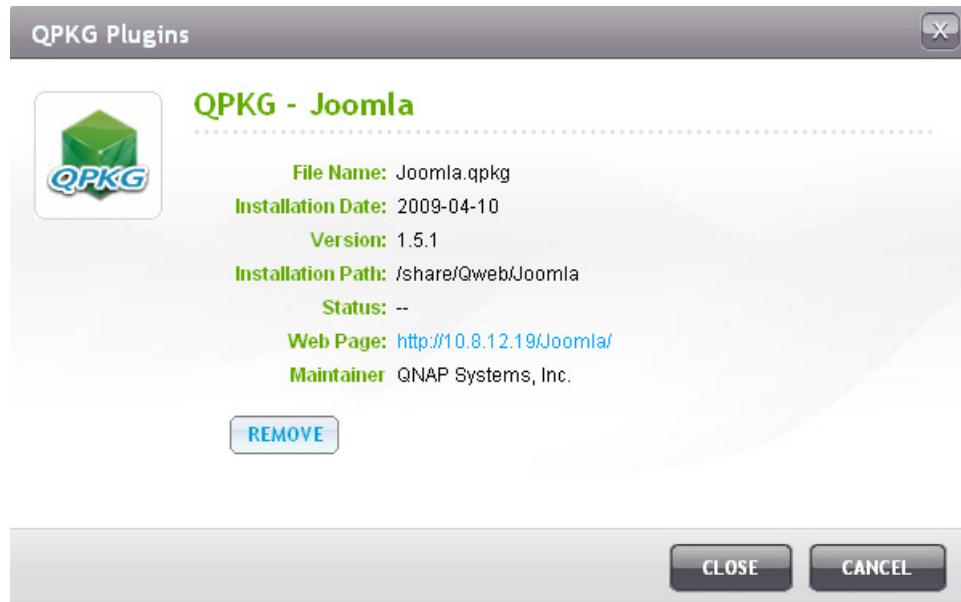
You can install QPKG packages to add more functions to NAS. Click "GET QPKG".



Before you install the packages, make sure the files are correct, read the instructions carefully, and back up all important data on the NAS. Download the software package you want to install on NAS to your computer.  
Before installing the QPKG package, please unzip the downloaded file. To install QPKG, browse to select the correct qpkg file and click "INSTALL".



After uploading the QPKG packages, the details are shown on the QPKG page. Click the link to access the web page of the installed software package and start to configure the settings. To remove the package from the NAS, click "REMOVE".



## 3.6 Backup

Home >> Backup

### Backup



External Drive



USB One Touch Copy



Remote Replication

#### 3.6.1 External Drive

### External Drive

#### Back up to an external storage device

Back up the local disk data to an external storage device. You can select instant, automatic, or schedule backup.

##### Directory to back up



##### Directory not to back up

- Network Recycle Bin 1
- Public
- Qdownload
- Qmultimedia
- Qrecordings
- Qusb
- Qweb

Back up to an External Storage Device:  No external device is detected currently.

Free Size/Total Size:--

Backup Method:  Do not execute any backup.

Copy options:  Back up data to the destination drive.

Current Backup Status: No backup operations.

Last Backup Time:

Last Backup Result:

You can back up the local drive data to an external storage device. In this page, you can select to execute instant, automatic, or schedule backup methods, and configure the relevant settings.

- **Backup Now:** To back up data to the external storage device immediately.
- **Schedule Backup:** To back up data by schedule. You can select the week day and time to execute the backup.
- **Auto-backup:** To execute the backup automatically once the storage device is connected to the NAS.

#### **Copy Options:**

You can select “Copy” or “Synchronize” for the copy options. When “Copy” is selected, files are copied from the NAS to the external device. By selecting “Synchronize”, the data on the internal drives of the NAS and the external storage device are synchronized. Any different files on the external device are deleted.

**Note:** In the copying and synchronizing process, if the identical files exist on both sides, the files are not copied. If there are files in the same name but different in size or modified dates on NAS and the external device, the files on the external device are overwritten.

### 3.6.2 USB One Touch Copy

You can configure the function of the USB one touch copy button in this page. The following three functions are available:

- Copy from the front USB storage to a directory of the internal drive of the NAS.
- Copy to the front USB storage from a directory of the internal drive of the NAS.
- Disable the one touch copy button

#### USB One Touch Copy

Configure the function of the USB one touch copy button.

Copy from the front USB storage device to the  directory of the internal disk.  
Backup method:  Back up data to the newly created directory on the destination sharing folder

Copy to the front USB storage device from the  directory of the internal disk.

Disable one touch copy button

**Note:** The USB LED blinks when data backup to an external device is in process. The USB one touch copy button will be disabled temporarily. If you press the button during the data transfer process, the server will beep thrice to alert you the button is disabled. Please wait for the backup to finish and the USB LED to stop flashing, and then use the USB one touch copy button again.

**APPLY**

#### Data Copy by the Front USB Port

The NAS supports instant data copy backup from the external USB device to the NAS or the other way round by the front one touch copy button. To use this function, follow the steps below:

1. Make sure a hard drive is installed and formatted on the NAS. The default network share Qusb is created.
2. Turn on the NAS.
3. Configure the behavior of the Copy button on "Backup" > "USB one touch copy" page.
4. Connect the USB device, e.g. digital camera or flash, to the front USB port of the NAS.
5. Press the Copy button (3 seconds). The data will be copied according to your settings on the NAS.

**Note:** Incremental backup is used for this feature. After the first time data backup, the NAS only copies the changed files since the last backup.

### 3.6.3 Remote Replication (Disaster Recovery)

You can use this option to back up the files on the NAS to another QNAP NAS or Rsync server over LAN or the Internet.

**Make sure a network share is created before creating a remote replication task.**

- ✓ **Port Number:** Specify a port number for remote replication. The default port number is 873.

**Note:** If this server connects to the Internet via a router, make sure the specified port for remote replication is opened on the router.

- ✓ **Enable backup from a remote server to the local host:** Check this option to allow the remote server to back up data to the local host via remote replication.
- ✓ **Allow remote Rsync server to back up data to NAS:** Enable this option to allow a remote Rsync server to back up data to the NAS by remote replication.

Remote Replication

Remote Replication

By using this function, you can back up the data on the local server to a remote server of the same NAS series, and also allow backup from remote server to the local server.

Port Number:

Enable backup from a remote server to the local host.

Allow remote Rsync server to back up data to NAS

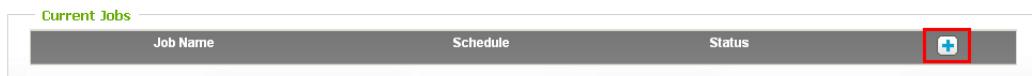
APPLY

Current Jobs

Job Name	Schedule	Status	+
----------	----------	--------	---

Follow the steps below to create a remote replication job for backup from the NAS to another QNAP NAS

- a. Click “+” to create a new task.

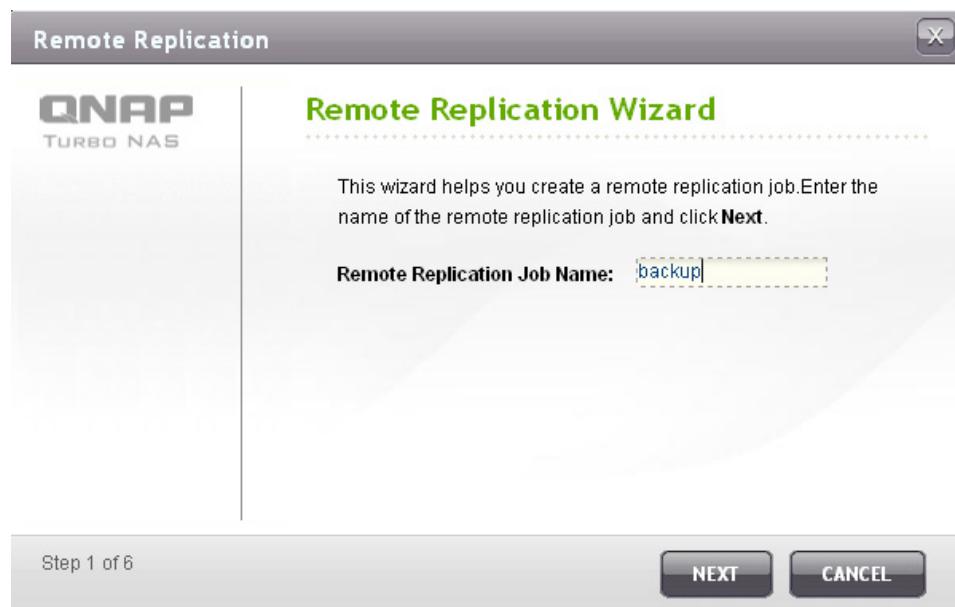


- b. Enter the job name and the remote destination settings. Select the server type.

Enter the IP address or domain name (if any) of the remote server, the port number of the remote server for remote backup, the destination path, and the user name and password with write access to the remote server. Click “Test” to check if the connection is successful or not.

**Note:**

- To use remote replication, enable Microsoft Networking service, make sure the destination network share and directory have been created, and the user name and password are valid to login the destination folder.
- The share folder name (network share or directory) is case-sensitive.



## Remote Destination

Server type:

Name or IP address of the remote server:  Port Number:

Destination Path (Network Share/Directory):

User Name:

Password:

Remote Host Testing:

- c. Enter the source path. You can select to back up the whole network share and a folder in the share. Then select to replicate data now or set a replication schedule.

## Local Source

Please specify: Local Source Path (Network Share/Directory)

/

## Replication Schedule

Select schedule:

Replicate Now

Daily

Weekly

Monthly   :

Time

- d. Set up other options for the remote replication job. Then click "Finish".

## Replication Options

Enable encryption, port number:

(Note that you have to allow SSH encryption on the remote host server and the port number must be the same as the SSH port of the remote host.)

Activate file compression

Stop network file services while replicating

Perform incremental replication

Delete extra files on remote destination

You can view the backup status, or edit or delete the replication job.

Current Jobs			
Job Name	Schedule	Status	
backup	11:25 - Replicate Now	Finished(11:25 2009/4/14)	 

## 3.7 External Device

Home>> External Device

### External Device



External Storage Device



USB Printer



UPS Settings

#### 3.7.1 External Storage Device

The NAS supports USB disks and thumb drives for extended storage. Connect the USB device to the USB port of the NAS, when the device is successfully detected, the details are shown on this page.

It may take tens of seconds for the NAS server to detect the external USB device successfully. Please wait patiently.

Home>> External Device>> External Storage Device

Welcome

### External Storage Device

#### External Storage Device

Manufacturer: --

Model: --

Device Type: --

Total / Free size: --

File System: --

Status: No disk

Format As: EXT 3

Eject:

To remove the hardware device, please click [Eject now]. When the system does not show the device anymore, you can remove it safely.

**Note:** Do NOT unplug the device when it is in use to protect the device.

### 3.7.2 USB Printer

To provide printer sharing function for the network users, you can simply connect a USB printer to the USB port of the NAS. The NAS detects the printer automatically. Up to 3 printers are supported.



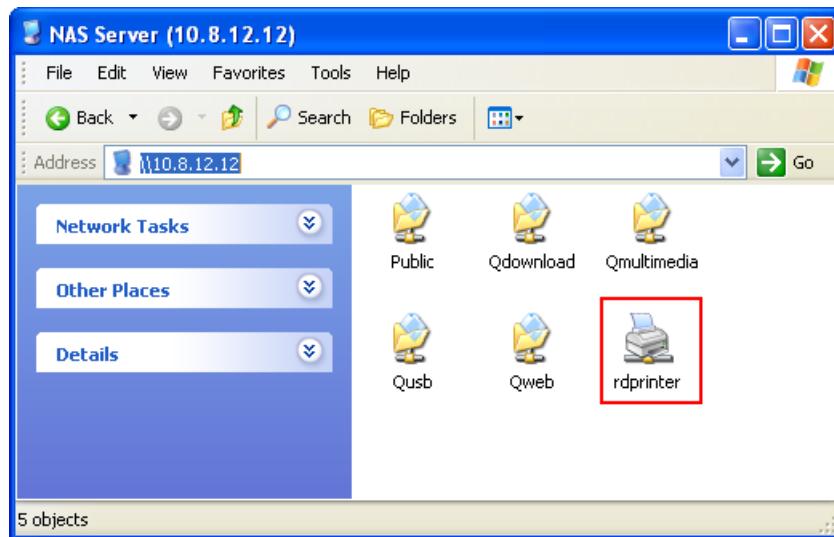
**Note:**

- Please connect a USB printer to the server after the software configuration is completed.
- The NAS does not support multifunction printer.
- For the information of supported USB printer models, please visit <http://www.qnap.com>.

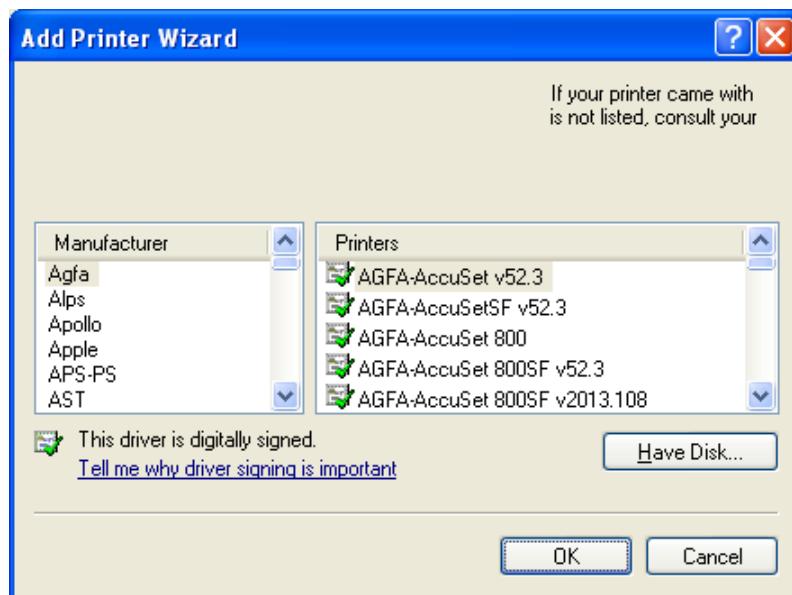
### **3.7.2.1 Windows XP Users**

#### **Method 1**

1. Enter \\NAS IP in Windows Explorer.
2. A printer icon is shown as a network share on the server. Double click the icon.



3. Install the printer driver.



4. When finished, you can start to use the network printer service of the NAS.

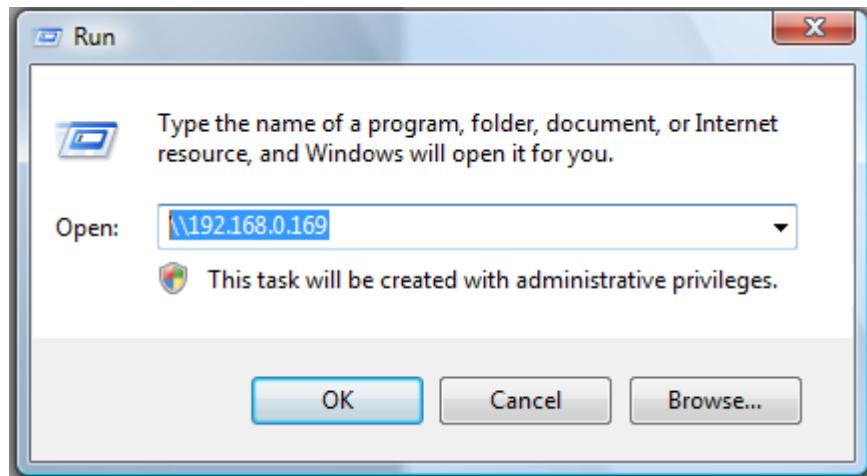
## **Method 2**

The following configuration method has been verified on Windows XP only:

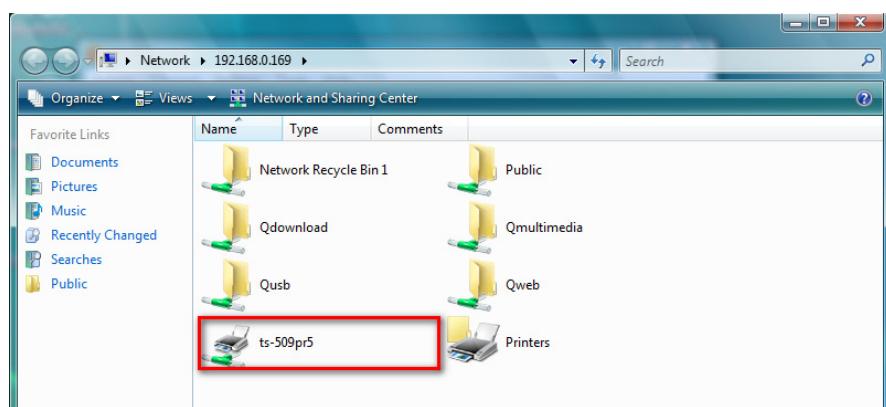
1. Open "Printers and Faxes".
2. Delete the existing network printer (if any).
3. Right click the blank area in the Printers and Faxes window. Select "Server Properties".
4. Click the "Ports" tab and delete the ports configured for the previous network printer (if any).
5. Restart your PC.
6. Open Printers and Faxes.
7. Click "Add a printer" and click "Next".
8. Select "Local printer attached to this computer". Click "Next".
9. Click "Create a new port" and select "Local Port" from the drop-down menu. Click "Next".
10. Enter the port name. The format is \\NAS IP\NAS namepr, e.g. NAS IP= 192.168.1.1, NAS name= myNAS, the link is \\192.168.1.1\myNASpr.
11. Install the printer driver.
12. Print a test page.

### **3.7.2.2 Windows Vista Users**

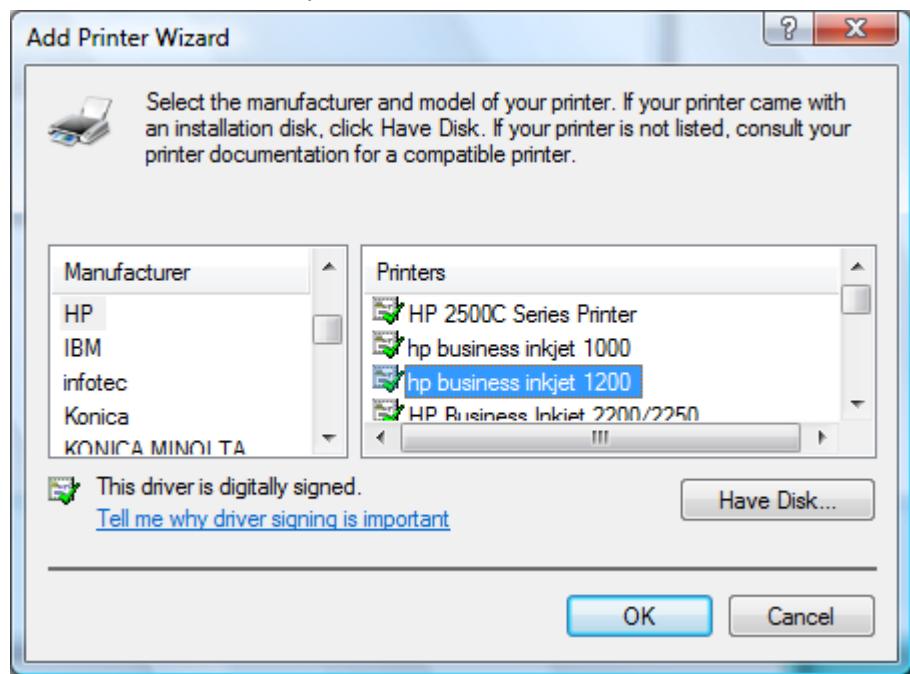
1. On the Run menu, enter \\NAS IP.



2. Find the network printer icon and double click it.



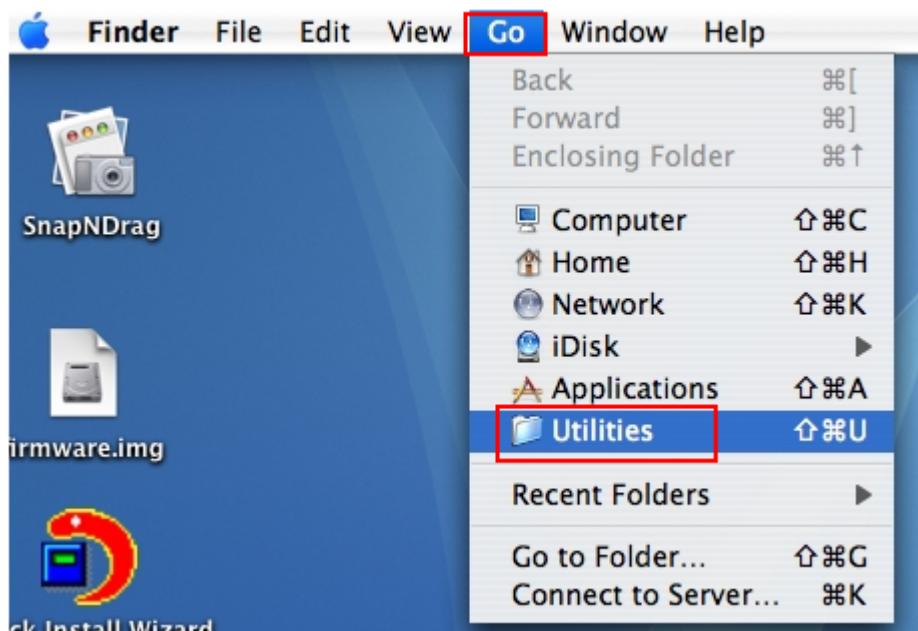
3. Install the correct printer driver.



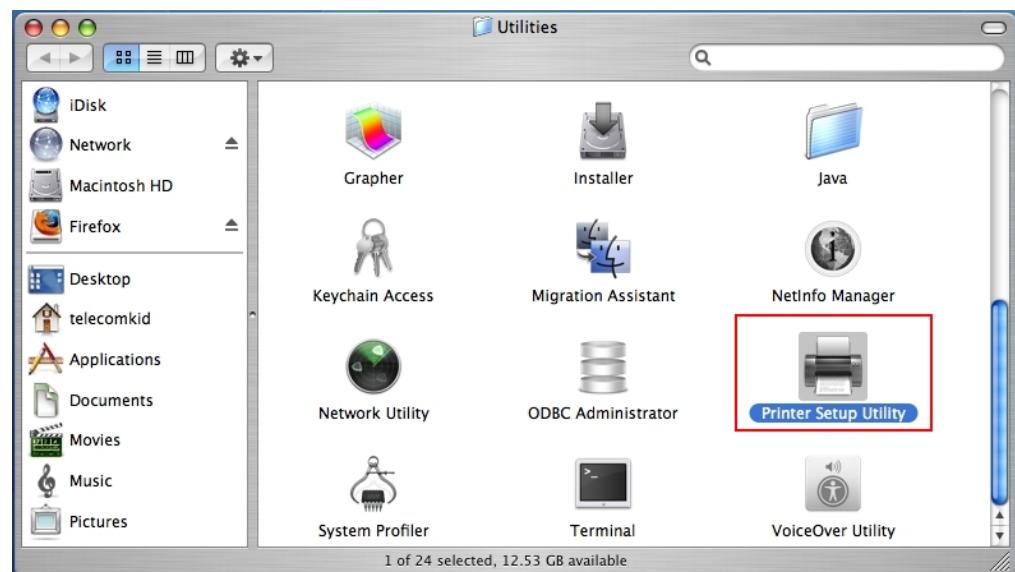
4. When finished, print a test page to verify the printer is ready to use.

### 3.7.2.3 Mac Users

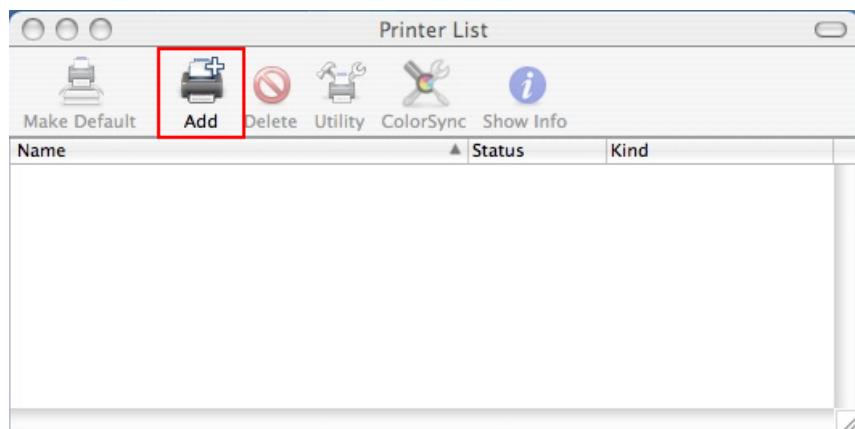
1. On the toolbar, click "Go/ Utilities".



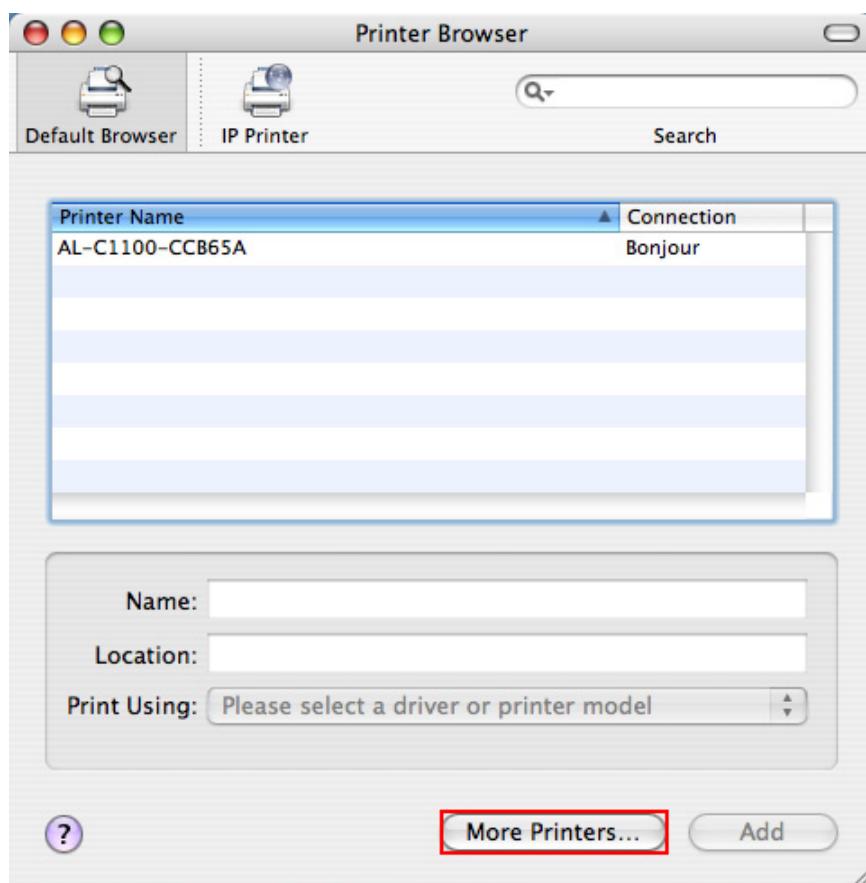
2. Click "Printer Setup Utility".



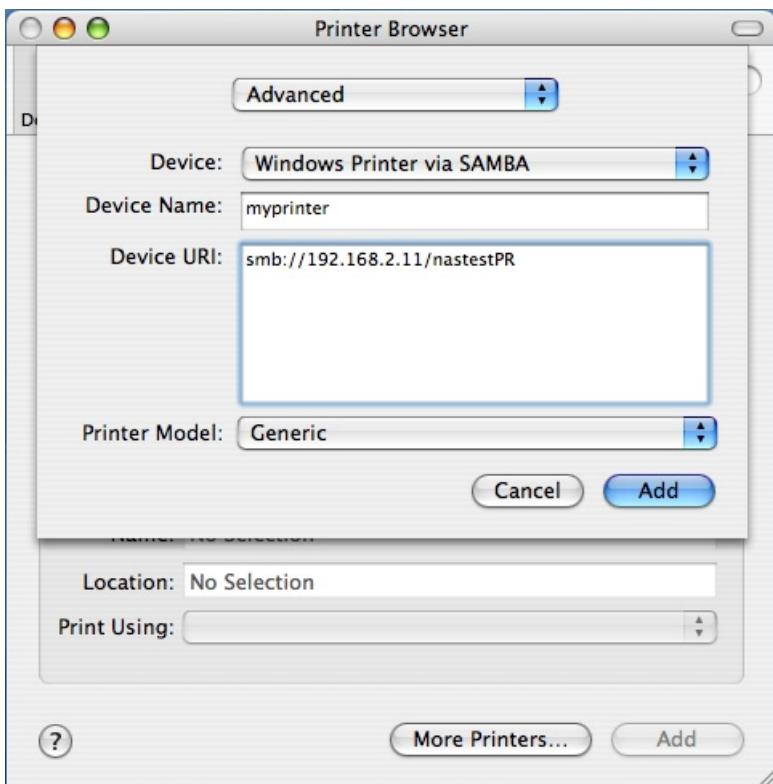
3. Click "Add".



4. Press and hold the "alt" key  on the keyboard and click "More Printers" concurrently.

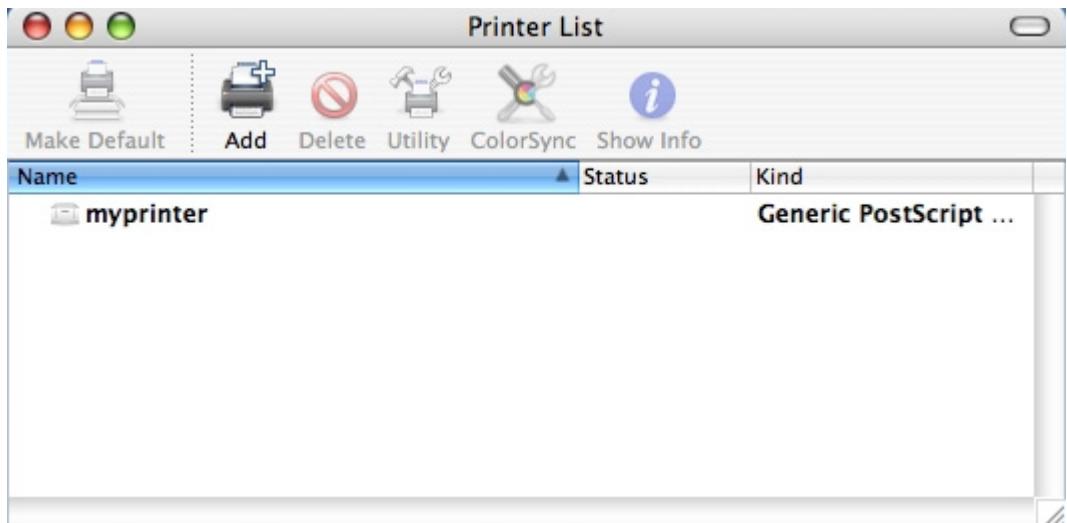


5. In the pop up window:
  - a. Select "Advanced"\*.
  - b. Select "Windows Printer with SAMBA".
  - c. Enter the printer name.
  - d. Enter the printer URI, the format is smb://NAS IP/printer name. The printer name is found on the "Device Configuration" > "USB Printer page".
  - e. Select "Generic" for Printer Model.
  - f. Click "Add".



\*Note that you must hold and press the "alt" key and click "More Printers" at the same time to view the Advanced printer settings. Otherwise, this option does not appear.

6. The printer appears on the printer list. It is ready to use.



**Note:** The network printer service of the NAS supports Postscript printer on Mac OS only.

### 3.7.3 UPS Settings

If your UPS device provides USB interface, you can enable UPS (uninterruptible power supply) support to protect your system from abnormal system shutdown caused by power outage.

The screenshot shows two sections of a server configuration interface:

- UPS Settings**:
  - Enable UPS Support
    - After the AC power fails for  minute(s) when the AC power status is abnormal.
    - After the AC power fails for  minute(s), the server should enter standby mode. When the power resumes, the system resumes to the operation status.
  - UPS Model:
  - IP Address of UPS:
- UPS Information**:
  - UPS Brand: --
  - UPS Model: --
  - AC Power Status: --
  - Battery Capacity: --
  - Estimated Protection Time: --

#### ✓ **Enable UPS support**

To activate the UPS support, you can select this option. You can set the shutdown timer to turn off the system automatically after the system detects the AC power is abnormal. In general, the UPS can keep supplying the power for the system for about 5~10 minutes, depending on the maximum load of the UPS and the number of the loads connected to it. You may also configure the system to enter standby mode in case of abnormal AC power supply.

#### ✓ **UPS Model**

Select the UPS model from the list. If the UPS model you are using is not available on the list, please contact our technical support.

#### ✓ **IP Address of UPS**

If you have selected APC UPS with SNMP for UPS model, enter the IP address of the UPS.

## 3.8 System Status

Home>> System Status

### System Status



System Information



Network Settings



Resource Monitor

#### 3.8.1 System Information

You can view the system information, e.g., CPU usage and memory on this page.

### System Information

#### System Information

CPU Usage	1.8 %
Total Memory	503.5 MB
Free Memory	450.4 MB
Packets Received	962720
Packets Sent	640610
Error Packets	0
System temperature	45° C/113° F
HDD 1 temperature	38° C/100° F
HDD 2 temperature	41° C/105° F
System Up Time	0 Day 0 Hour 57 Minute(s)

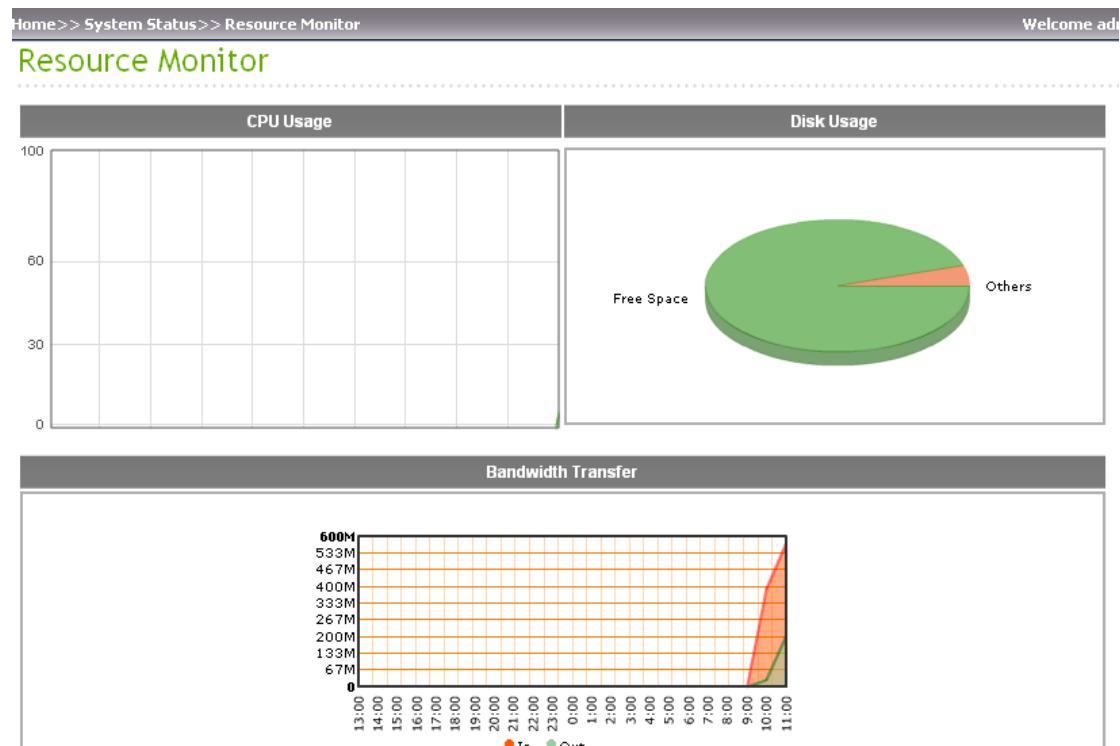
### 3.8.2 System Service

You can view current network settings and status of the NAS in this section.

System Service	
<b>Microsoft Networking</b>	
Enabled	●
Server Type	Standalone Server
Workgroup	QATEST
Enable WINS server	○
Enable Domain Master	○
<b>Apple Networking</b>	
Enabled	●
Apple Zone Name	*
<b>Unix/Linux NFS</b>	
Enabled	●
<b>Web File Manager</b>	
Enabled	●
<b>FTP Service</b>	
Enabled	●
Port	21
Maximum Connections	30
<b>Multimedia Station</b>	
Enable Multimedia Station	●
Enable iTunes Service	●
Enable UPnP Media Server	○
<b>Download Station</b>	
Enabled	●
<b>Web Server</b>	
Enabled	○
Port	80
register_globals	●
<b>DDNS Service</b>	
Enabled	○
<b>MySQL Server</b>	
Enabled	●
Enable TCP/IP Networking	●
<b>System Port Management</b>	
Port	8080

### 3.8.3 Resource Monitor

You can view the CPU usage, disk usage, and bandwidth transfer statistics of the NAS on this page.



# Chapter 4    Multimedia Station

## 4.1    Share Photos and Multimedia Files via the Web Interface

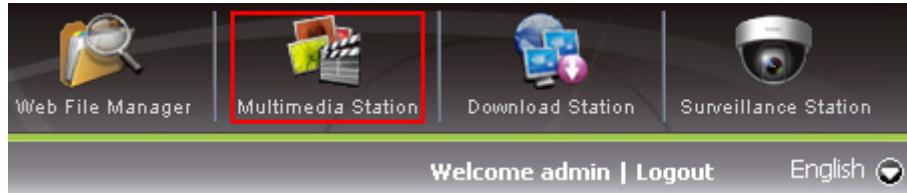
The NAS provides a user-friendly web management interface for you to manage personal albums easily. You can view images and multimedia files, or browse photos by thumbnails preview.

### A. Upload photos by web administration

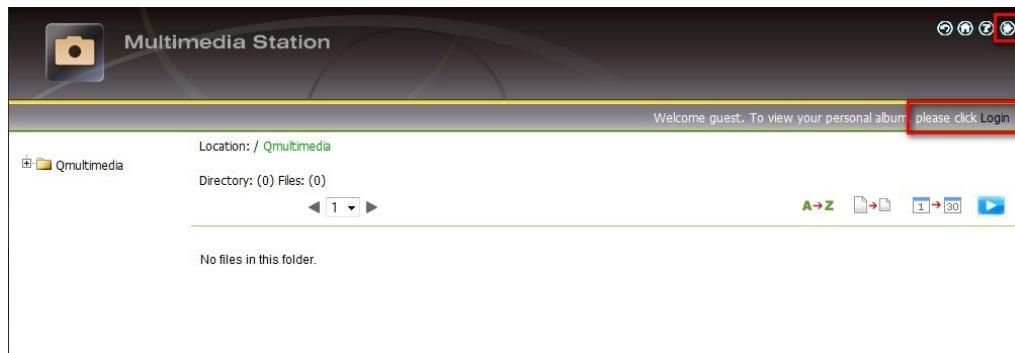
1. Go to "Applications" > "Multimedia Station". Enable the service.

The screenshot shows a web-based configuration interface for the Multimedia Station. At the top, there is a navigation bar with links for Home, Applications, and Multimedia Station. On the right side of the bar, there are links for Welcome admin | Logout and English. Below the navigation bar, the title "Multimedia Station" is displayed in green. A sub-menu titled "Multimedia Station" is open, showing two configuration options: "Enable Multimedia Station" (which is checked) and "Show service link on the login page." At the bottom right of the configuration area, there is a blue "APPLY" button.

2. Click “Multimedia Station” on the top or on the login page of the NAS to access the Multimedia Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.



3. Click “Login” on the top right hand corner. Login with administrator name and password to manage the Multimedia Station. You can create user accounts to allow the users to access the multimedia files.



4. Click “Browse” to select the multimedia file and then click “Upload” to upload the file to the folder.

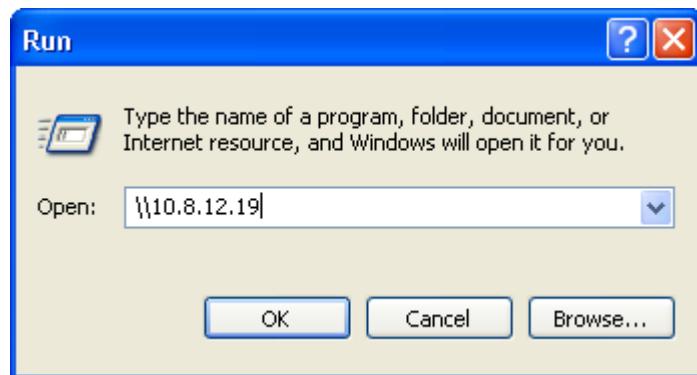


5. You can also create folders by clicking and upload the files to the folders.

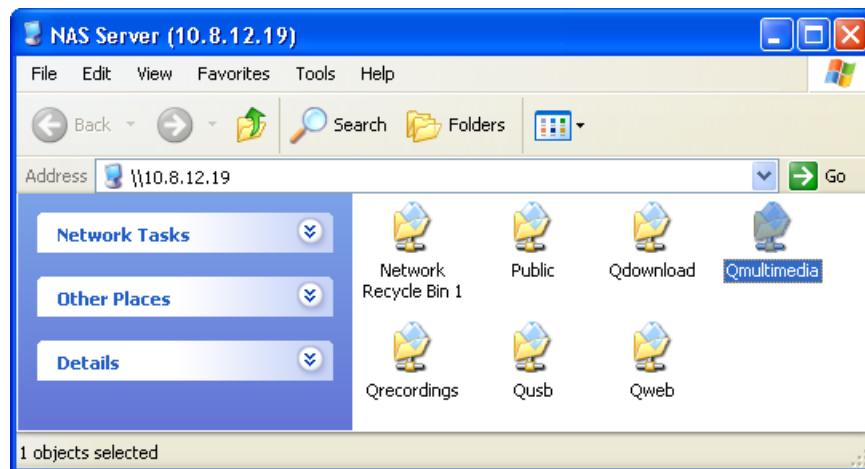
## **B. Upload photos to Qmultimedia folder directly**

You can upload multimedia files to the NAS directly by the following steps.

1. Open the Windows Run menu. Enter \\[server name] or \\[server IP] to access share folder on the NAS.

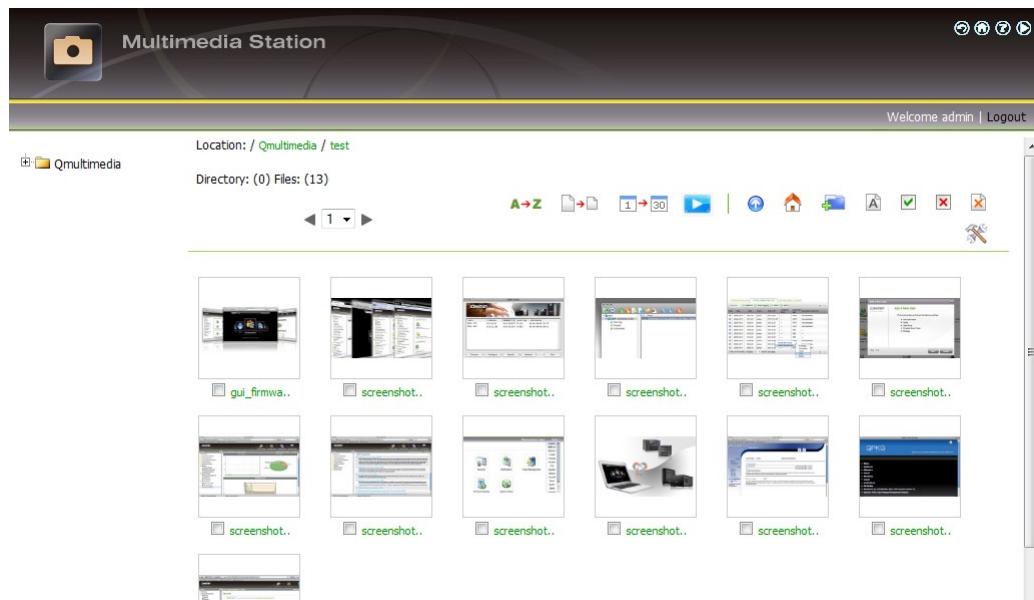


2. Open the folder Qmultimedia. Enter the user name and password to login.



3. Drag the files and folders to the folder directly. Please wait patiently when the NAS is generating thumbnails for images during uploading.

When you login Multimedia Station by web browser again, all the multimedia files will be shown.



### **Buttons on the Multimedia Station page**

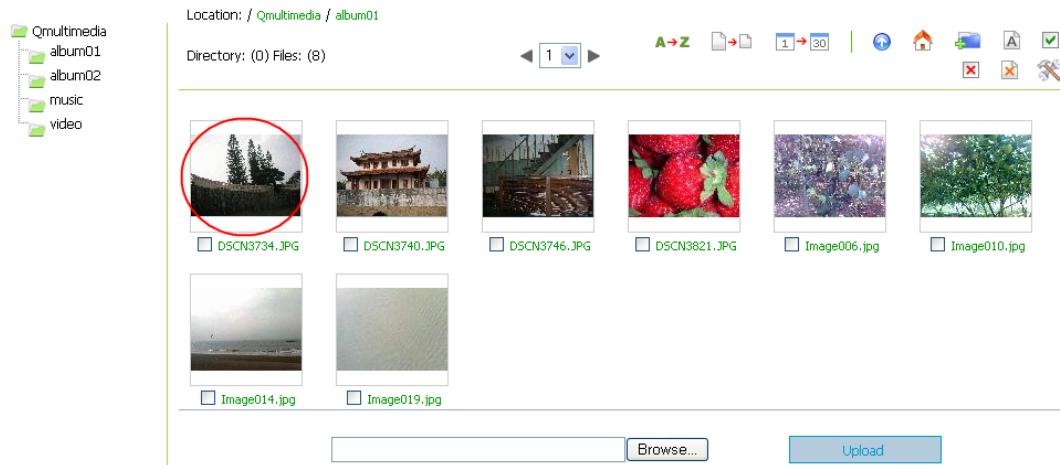
	Sort files by name
	Sort files by size
	Sort files by date
	Return to previous page
	Return to Home
	Create folder
	Rename file or folder
	Select all
	Select none
	Delete

### **Support file format list**

Type	File format
Picture	jpg, bmp, gif
Video	wmv, wmx, wvx, avi, mpeg, mpg, mpe, m1v, mp2, mpv2, mp2v, mpa, dvr-m, asf, asx, wpl, wm, wmx, wmd, w mz
Audio	wma, wax, cda, wav, mp3, m3u, mid, midi, rmi, aif, aifc, aiff, au, snd
Others	(Other formats not mentioned above)

## View Photo Information

1. To view detailed information of a photo, click the thumbnail of the picture.



2. The information of the photo, e.g. file name, resolution, size, camera producer will be shown on the right. You can enter a description for the picture in the box below the photo and click "Submit". To reset the description to previously saved version, click "Reset".



## **Buttons Description**

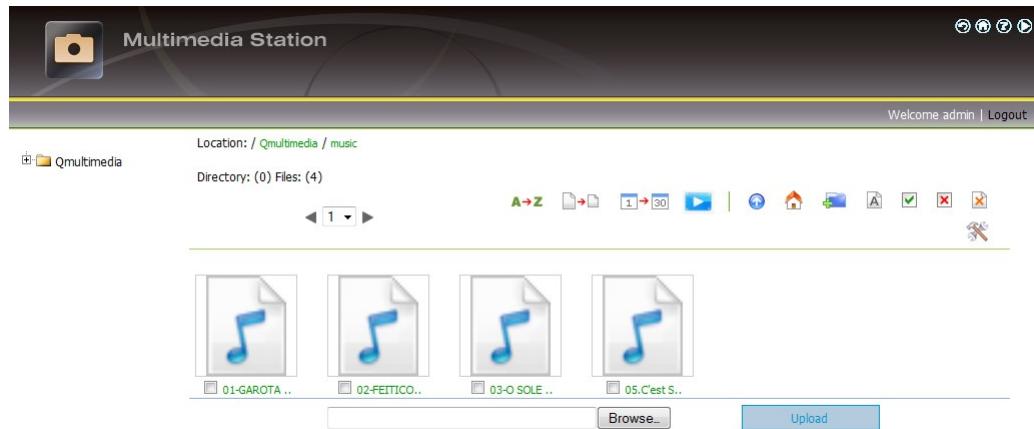
You can use the buttons on top of the photo to manage the album.

	Back to previous level
	Previous image
	Next image
	Rotate image anticlockwise
	Rotate image clockwise
	Zoom in
	Zoom out
SlideShow:	Play slideshow. Select the time interval in seconds. Click "play" to play slide show. To stop playing, click "stop".
	Print the image
	Save the picture
	Set the picture as album cover

## Play music or video files

To play music or video files on the Multimedia Station, you can click the thumbnail of the file displayed on the page. The file will be played by the default music or video playing program of your PC.

\*It is recommended to use Windows Media Player 10.0 or above as the default playing program.

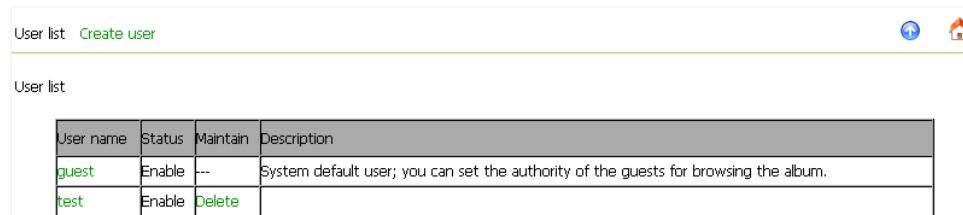


### C. Configure album authority

1. After logging in as administrator (admin), click  to enter the configuration page for album authority.



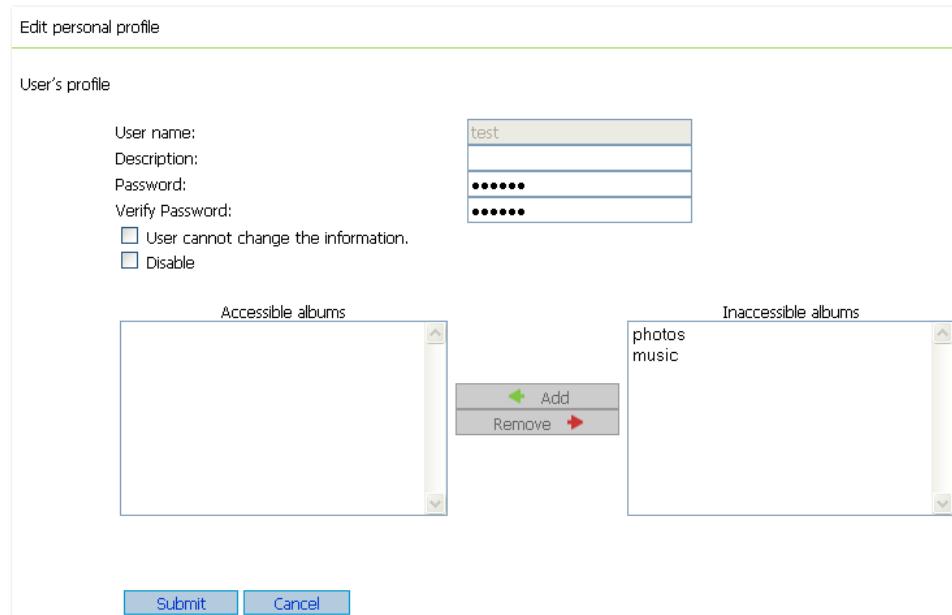
2. You can view, add, delete, and edit users.



The screenshot shows the 'User list' configuration page. At the top, there are tabs for 'User list' and 'Create user'. Below the tabs is a search bar and a refresh button. The main area is titled 'User list' and contains a table with two rows:

User name	Status	Maintain	Description
guest	Enable	---	System default user; you can set the authority of the guests for browsing the album.
test	Enable	<a href="#">Delete</a>	

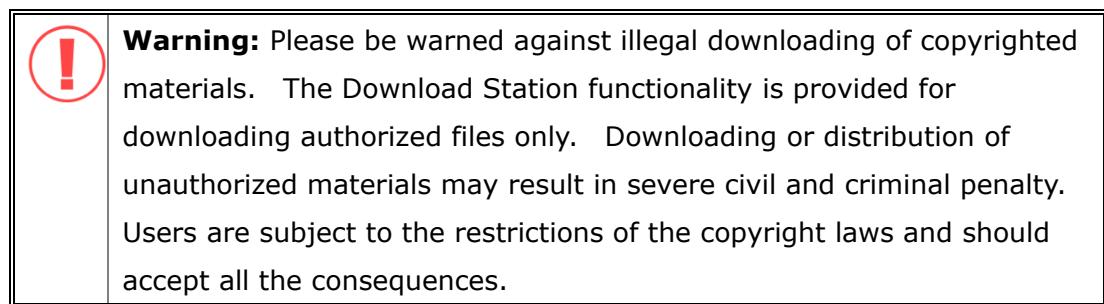
3. You can edit the user profile and album access authority on this page.



The screenshot shows the 'Edit personal profile' configuration page. At the top, there's a header 'Edit personal profile'. Below it, a section titled 'User's profile' contains fields for 'User name' (set to 'test'), 'Description' (empty), 'Password' (empty), and 'Verify Password' (empty). There are also checkboxes for 'User cannot change the information.' and 'Disable'. To the right of these fields is a password strength meter showing four dots. Below this is a section titled 'Accessible albums' which is currently empty. To its right is a section titled 'Inaccessible albums' containing 'photos' and 'music'. Between the two sections is a central panel with 'Add' and 'Remove' buttons. At the bottom are 'Submit' and 'Cancel' buttons.

## Chapter 5 Download Station

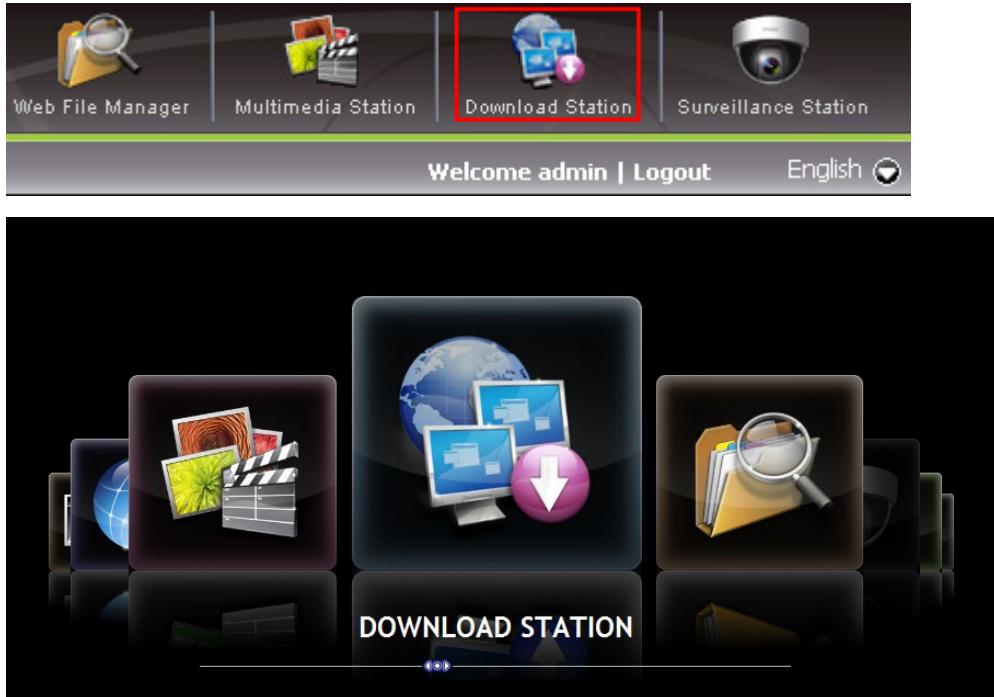
The NAS supports BT, HTTP, and FTP download. You can add download task to the NAS and let the server finish downloading independent of PC.



1. Go to "Applications" > "Download Station". Enable the service.

Screenshot of the "Download Station" configuration page. The URL is "Home >> Applications >> Download Station". The top right shows "Welcome admin | Logout" and "English". The main title is "Download Station". A sidebar on the left lists "Download Station". Under "Download Station", there are two checked checkboxes: "Enable Download Station" and "Show service link on the login page.". At the bottom right is a blue "APPLY" button.

- Click “Download Station” on the top or on the login page of NAS to access the Download Station. If you login the service from the login page of the NAS, you are required to enter the user name and password.

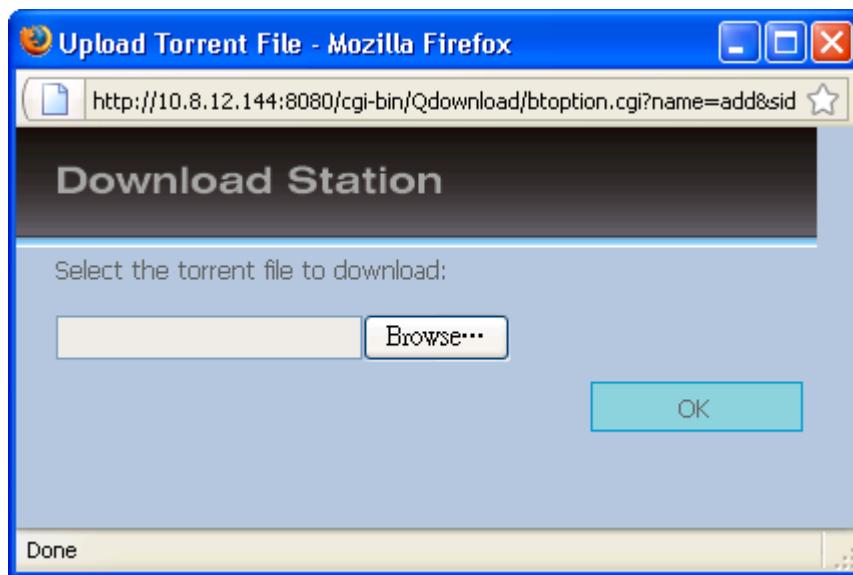


- Select Add new BT task or Add new FTP/HTTP task.

#### **(A) Add new BT task**

Click “Add new BT task” on the left and upload a torrent file. You can download legal torrent files by searching on the Internet. There are websites that provide legally sharing torrents e.g. [www.legaltorrents.com](http://www.legaltorrents.com). Please download the torrent files to your local disk and then upload them to the NAS.

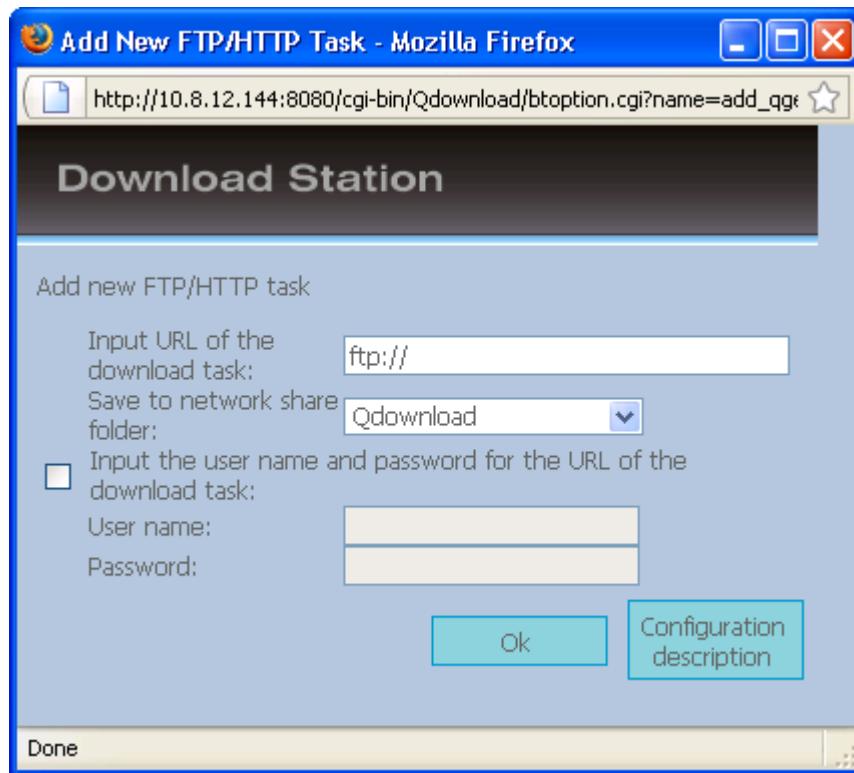
The image shows the 'Download Station' interface. At the top, there is a navigation bar with buttons for 'View Run List', 'View Pause List', 'View Finish List', and 'How to Use'. Below the navigation bar, there is a sidebar on the left with options: 'Add new BT task' (highlighted with a red box), 'Add new FTP/HTTP task', 'Pause/Rerun download task', 'Delete download task', 'BT download property', 'Set Config', and 'Dump Diagnostic Information'. To the right of the sidebar is a table titled 'Download task' with columns for Status, Size, %, Downloaded, Uploaded, SeedPeer, Time Left, Share rate, and DHT. A message 'No records found.' is displayed in the table area. At the bottom right of the interface, there are buttons for 'Increase download priority' and 'Decrease download priority'.



### (B) Add new FTP/HTTP task

To run an FTP download task, click "Add new FTP/HTTP task". Enter the FTP URL of the download task and select the share folder to save the files. Enter the user name and password to login the FTP server (if necessary). Then click "OK" to start downloading.

To run an HTTP download task, click "Add new FTP/HTTP task". Enter the HTTP URL of the download task and select the share folder to save the files. Then click "OK" to start downloading.



4. After uploading a download task, the task will appear on View Run List.

View Run List									
		View Run List		View Pause List		View Finish List		How to Use	
Increase download priority   Decrease download priority									
Download task	Status	Size	%	Download	Upload	SendPeer	Time Left	Share rate	DHT
alceeee.torrent	RUN	786.80 MB	0.0	0.0 KB/s	0.0 KB/s	0.0	99:99:99	00	On

5. You can select a download task and click "BT download property" to enable or disable DHT public network and configure the sharing time after download completes.

- :: Add new BT task
- :: Add new FTP/HTTP task
- :: Pause/Restart download task
- :: Delete download task
- BT download property**
- :: Set Config
- :: Dump Diagnostic Information

Download task	Status	Size	%
Edit Share Time - Mozilla Firefox	0		

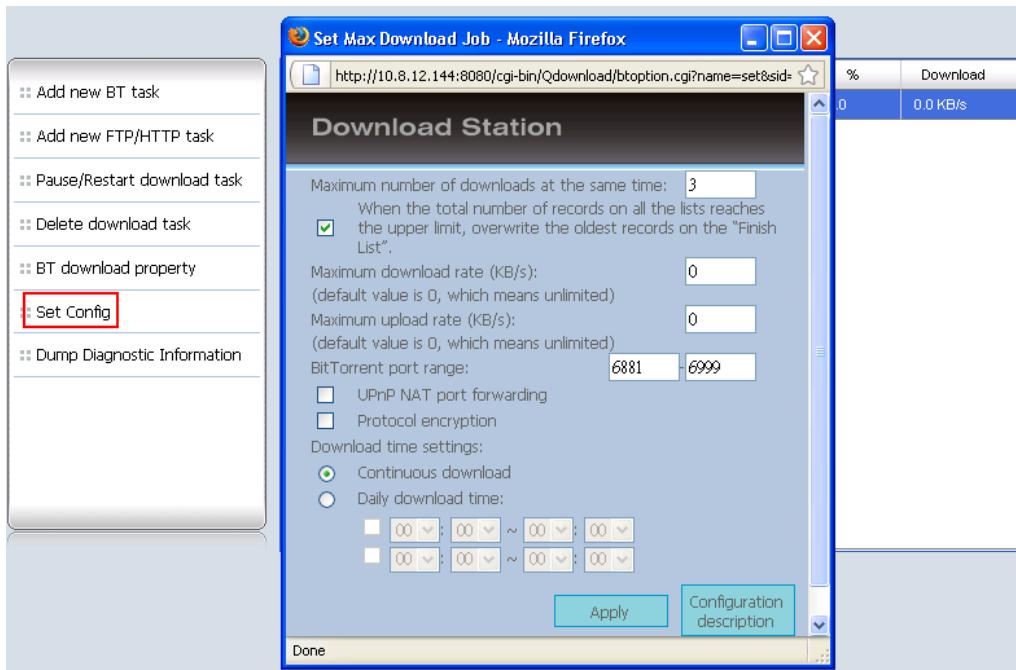
Sharing time after download task completes:  hr

Use public DHT network

**Apply**      Configuration description

**Note:** If the sharing time (larger than 0 hr) is set for a download task, the download task will be moved to Finish List after download completes and the sharing time ends.

- Click "Set Config" and enter the number of the maximum tasks you want to download at the same time (Default number: 3).  
Enter the maximum download rate (default value is 0, which means unlimited).  
Enter the maximum upload rate (default value is 0, which means unlimited).  
Enter the port range for Download Station (default range is 6881-6999).  
Check UPnP NAT port forwarding to enable automatically port forwarding on UPnP supported gateway (default is not checked).

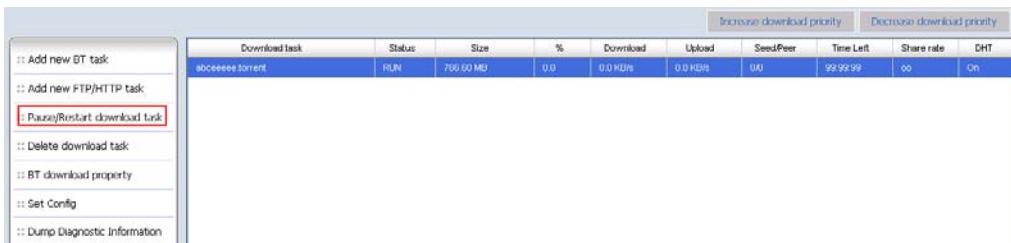


### Protocol Encryption

There are a number of Internet Service Providers (ISP) block or throttle BitTorrent connections for the high bandwidth it generates. By turning on "Protocol Encryption" your connections will not be distinguished by these ISPs as BitTorrent connections therefore are unable to block or throttle them and causing slow connections or even no connections. However some ISPs are starting to be able to identify these connections even if they were encrypted so users are suggested to check the Bad ISPs list on AzureusWiki and to consider switching to an ISP that does not perform BitTorrent traffic throttling or blocking.

You can set the download schedule in "Download time settings". Select "Continuous download" to download the files continuously. To specify the download schedule, select "Daily download time" and enter start and end time. If the end time value is smaller than the start time, the end time will be treated as the time on the next day.

7. To pause a running download task, select the task in View Run list and click "Pause/ Restart download task". You can view tasks that are paused or finished in View Pause List and View Finish List respectively. To restart a paused task, select the task in View Pause List and click "Pause/ Restart download task".



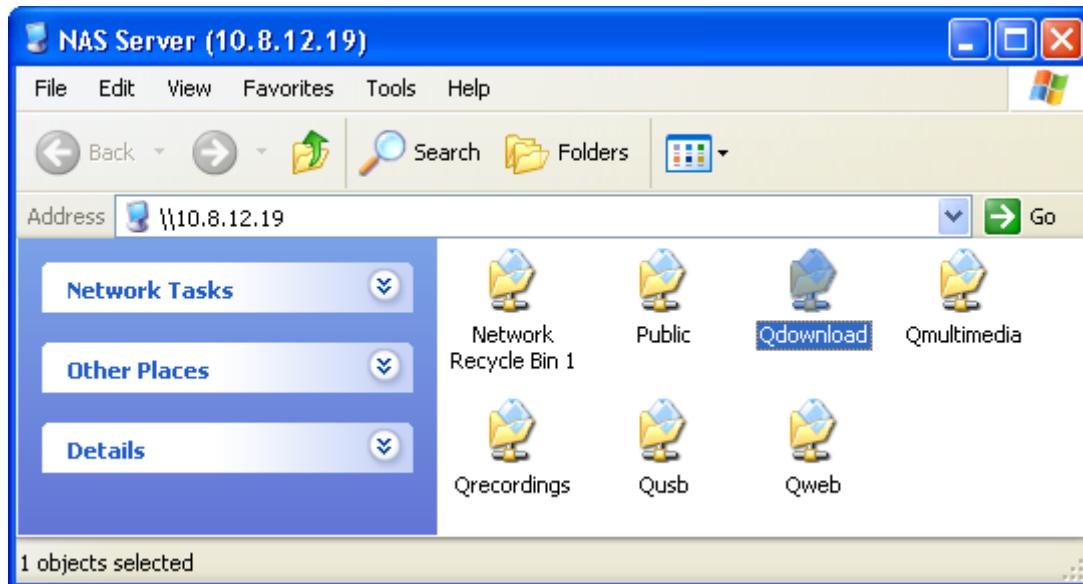
8. You can also increase or decrease task priority by clicking "Increase download priority" and "Decrease download priority" when there are multiple download tasks.



9. To delete a running, paused, or finished task, select the task and click "Delete download task". You can select to remove the download task only and retain the downloaded files, or remove the task and downloaded files.

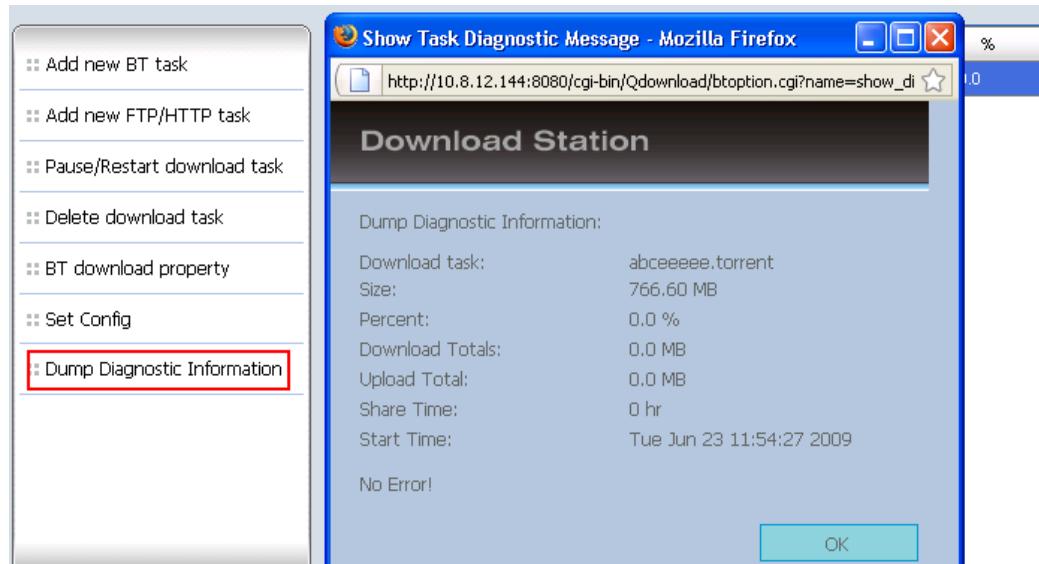


10. To logout Download Station, click  on the top right hand corner.
11. To access the folders you have downloaded, please go to the share folder Qdownload of the NAS.

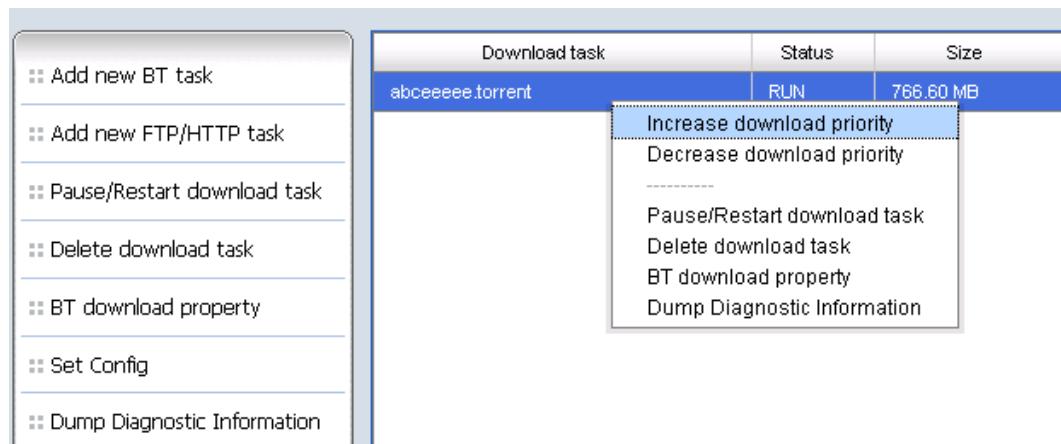


## Dump Diagnostic Information

To view the diagnostic details of a download task, select a task on the list and click "Dump Diagnostic Information".



You can right click the download task to configure the download settings.



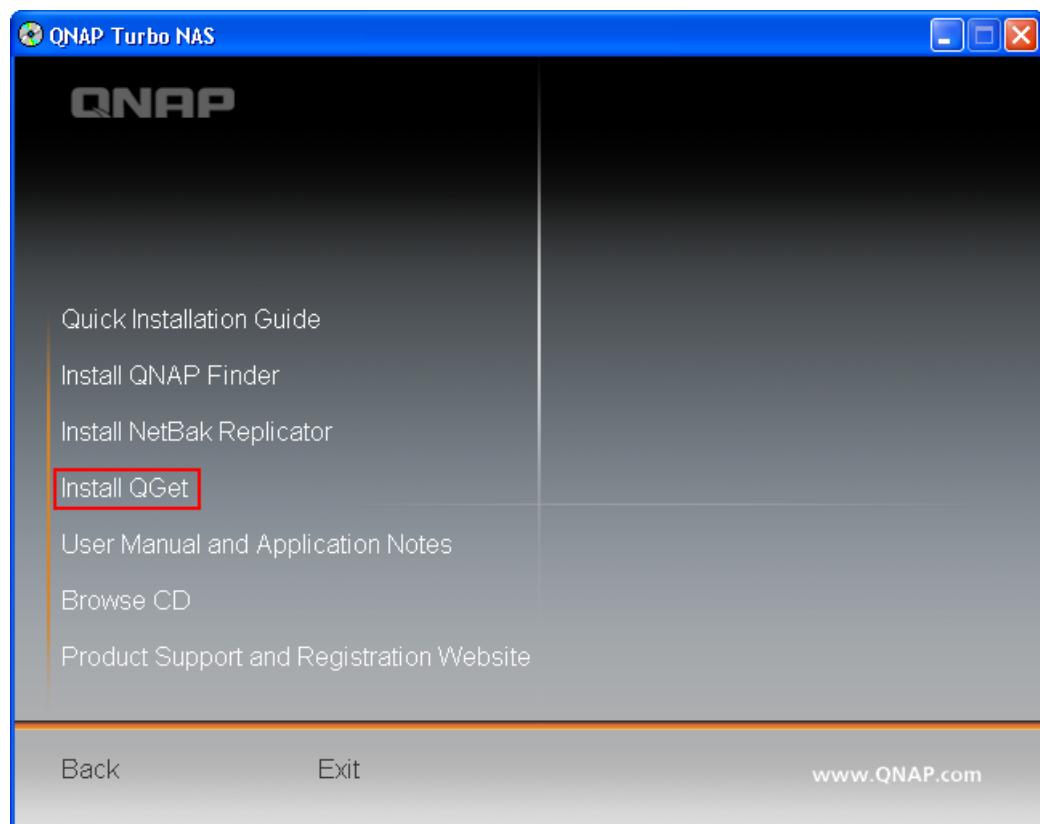
The common reasons for slow BT download rate or download error are as below:

- (1) The torrent file has expired, the peers have stopped sharing this file, or there is error in the file.
- (2) The NAS has configured to use fixed IP but DNS server is not configured, or DNS server fails.
- (3) Set the maximum number of simultaneous downloads as 3-5 for the best download rate.
- (4) The NAS is located behind NAT router. The port settings have led to slow BT download rate or no response. You may try the following means to solve the problem:
  - a. Open the BitTorrent port range on NAT router manually. Forward these ports to the LAN IP of the NAS.
  - b. The new NAS firmware supports UPnP NAT port forwarding. If your NAT router supports UPnP, enable this function on the NAT. Then enable UPnP NAT port forwarding of the NAS. The BT download rate should be enhanced.

## 5.1 Use Download Software QGet

QGet is a powerful management software for maintaining the BT, HTTP and FTP download tasks of multiple TS series NAS servers via LAN or WAN. By using QGet, you no longer need to login the Download Station web interface of multiple servers and manage the settings one by one. Simply install QGet on any computer running Windows 2000/XP or Mac, you can manage the download tasks of all your NAS servers.

1. To use QGet, install the software from the product CD-ROM.



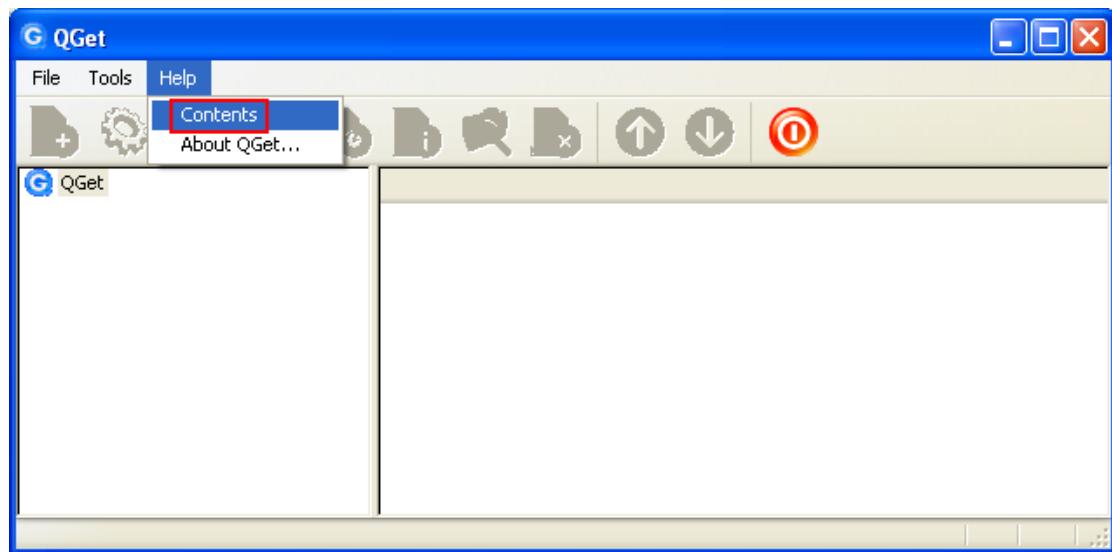
2. Follow the instructions to install QGet.



3. Run QGet from the installed location.



4. For the details of using QGet, please refer to the online help of the software.



# Chapter 6 Web Server

The NAS enables you to upload web pages and manage your own website easily by Web Server function. It also supports Joomla!, PHP and MySQL/SQLite for you to establish an interactive website.

1. Go to "Network Service" > "Web Server". Enable the service and enter the port number.

The screenshot shows the QNAP Web interface with the following details:

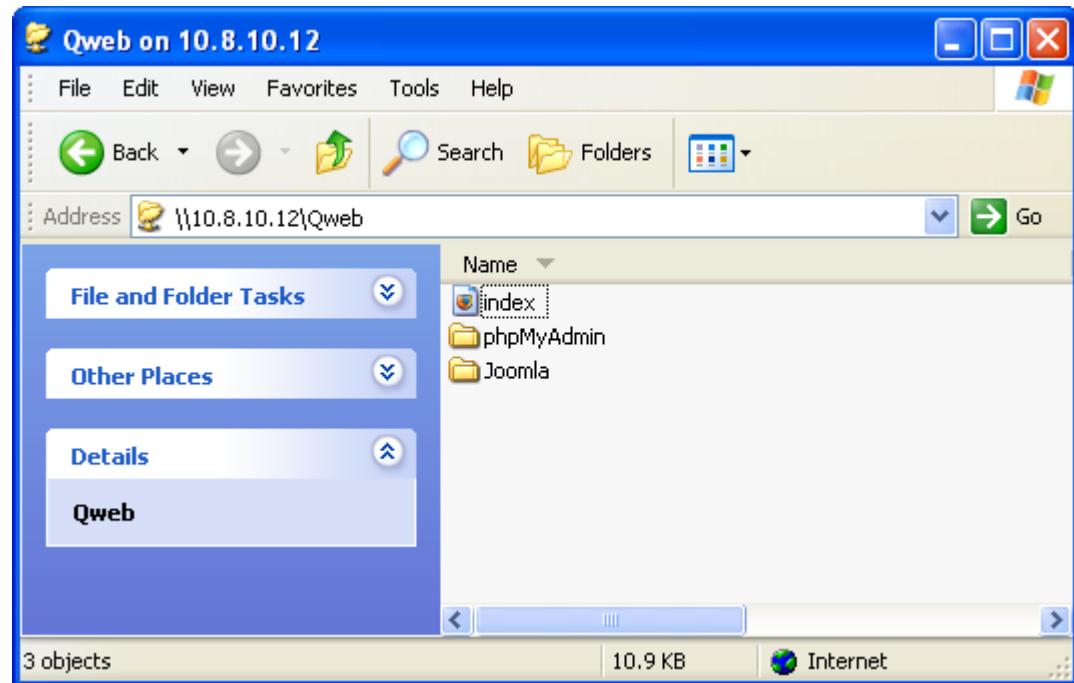
- Header:** Home >> Network Service >> Web Server | Welcome admin | Logout | English | ?
- Section:** Web Server
- Configuration:**
  - Enable Web Server (checkbox checked)
  - Port Number: 80
  - register\_globals: On (radio button)
- Note:** After enabling this service, click the following link to enter to Web Server.  
<http://172.17.20.39>
- Buttons:** APPLY

**php.ini Maintenance**

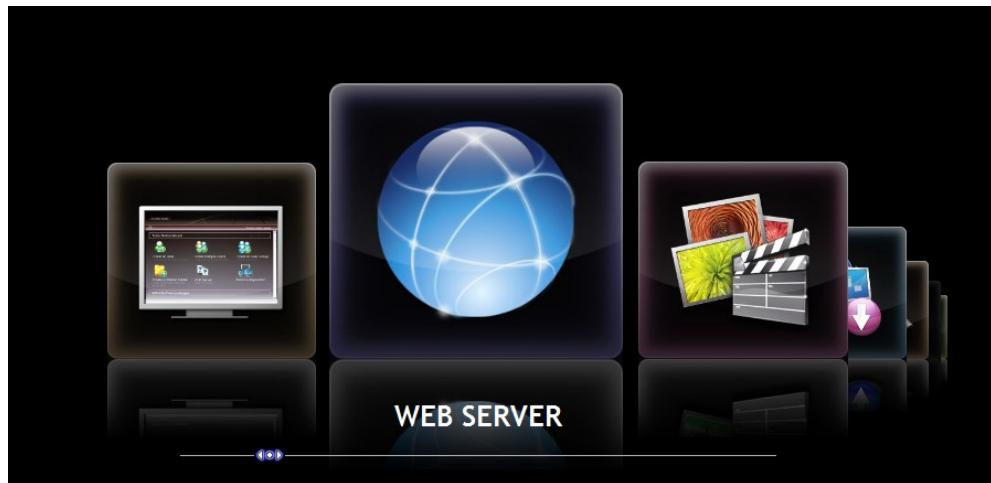
php.ini Maintenance  
The file **php.ini** is the system configuration file of Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended to use the system default setting.

2. You can upload your HTML files to the folder Qweb by the following methods:
- By using samba: You can open a web browser and type **\[NAS IP]\Qweb** or **\[NAS name]\Qweb**. Login the folder and upload your HTML files.
  - By FTP: You can login FTP service and upload your HTML files to the folder.
  - By Web File Manager: You can login Web File Manager and upload your HTML files to the folder.

The file index.html, index.htm or index.php will be the home path of your web page.



3. Click the link <http://NAS IP/> on Web Server page or click “Web Server” on the login page of the NAS to access the web page you upload. Note that when Web Server is enabled, you have to type [http://NAS IP address:8080] in your web browser to access the login page of the NAS.



For the online tutorial, please visit [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

## **MySQL Management**

The first time you install the system, the phpMyAdmin software is automatically installed as the MySQL management tool. When you update the firmware in the future, phpMyAdmin will not be re-installed and your data on the database will not be overwritten or changed.

The phpMyAdmin program files are created in the Qweb share folders. You can change the folder name and access the database by entering the URL in the browser. However, the link on the web management interface is not changed.

**Note:** The default user name of MySQL is "root". The password is "admin". Please change your root password immediately after logging in to the phpMyAdmin management interface.

## **SQLite Management**

SQLiteManager is a multilingual web-based tool to manage SQLite databases and can be downloaded from <http://www.sqlitemanager.org/>.

Please follow the steps below or refer to the INSTALL file in the downloaded SQLiteManager-\*.tar.gz<sup>?</sup> to install the SQLiteManager.

- (1) Unpack your download file SQLiteManager-\*.tar.gz.
- (2) Upload the unpacked folder **SQLiteManager-\*** to \\NAS IP\Qweb\.
- (3) Open your web browser and go to [http://NAS IP/SQLiteManager-\\*/](http://NAS IP/SQLiteManager-*/).

<sup>?</sup>: The symbol "\*" refers to the version number of SQLiteManager.

# Chapter 7    FTP Server

The NAS supports FTP service. To use FTP service, enable this function in "Network Service" and follow the steps below:

The screenshot shows the 'FTP Service' configuration page. At the top, there are navigation links: Home >> Network Services >> FTP Service, Welcome admin | Logout, and English (Change). Below the header, the title 'FTP Service' is displayed. The page is divided into three main sections: General, Connection, and Advanced.

**General**

- Enable FTP Service
- Protocol Type:  
 FTP (standard)  
 FTP with SSL/TLS (Explicit)
- Port Number:
- Unicode Support:  Yes  No
- Enable Anonymous:  Yes  No

**Note:** If your FTP client does not support Unicode, please select "No" for Unicode Support and select a supported filename encoding from [\[Filename Encoding\]](#) under [General Settings] so that the folders and files on FTP can be properly shown.

**Connection**

- Maximum Number of all FTP connections:
- Maximum Number of Connections For a Single Account:
- Enable FTP transfer limitation
  - Maximum upload rate (KB/s):  KB/s
  - Maximum download rate (KB/s):  KB/s

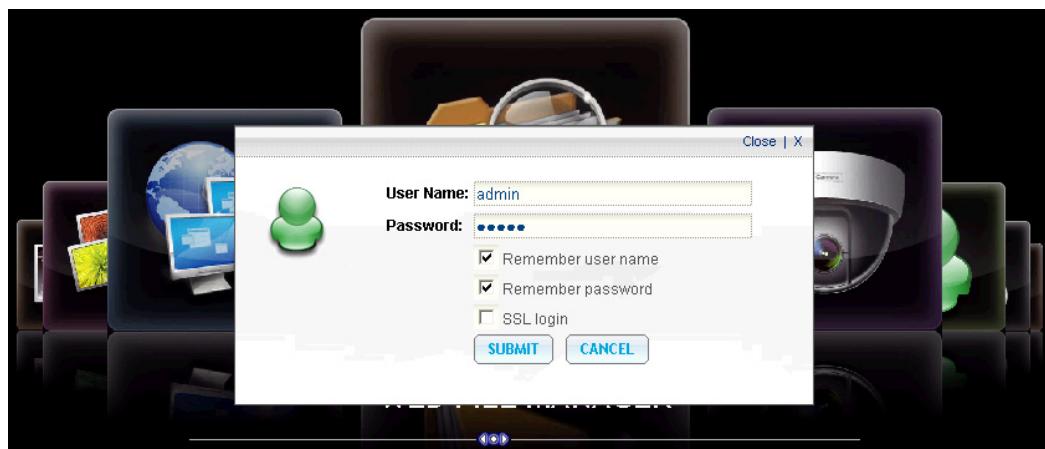
**Advanced**

- Passive FTP Port Range:  
 Use the default port range(55536 - 56559)  
 Define port range:  -

1. Open an IE browser and enter `ftp://[NAS IP]` or `ftp://[NAS name]`. OR

2. By Web File Manager of the NAS.

Go to NAS administration page and click "Web File Manager". Enter user name and password to login the NAS.



Click "FTP".

Share Folder	Comment
Network Recycle Bin 1	[Single Disk Volume: Drive 1]
Public	System default share
Qdownload	System default share
Qmultimedia	System default share
Qrecordings	System default share
Qusb	System default share
Qweb	System default share

Enter the user name and password to login FTP service. You can start to use FTP service.

## Chapter 8 Web File Manager

To use Web File Manager, go to “Applications” > “Web File Manager”. Enable the service.



Home >> Applications >> Web File Manager      Welcome admin | Logout      English 

Web File Manager 

**Web File Manager**

Enable Web File Manager

**APPLY**

Click “Web File Manager” on the top or on the login page of the NAS to access the Web File Manager. If you login the service from the login page of the NAS, you are required to enter the user name and password.

**Note:** Make sure a network share has been created before using Web File Manager.



Select a network share.

FTP		
	Ordner freigeben	Kommentar
	Network Recycle Bin 1	[Mirror Disk Volume: Drive 1 2]
	Public	System default share
	Qdownload	System default share
	Qmultimedia	System default share
	Qrecordings	System default share
	Qusb	System default share
	Qweb	System default share

You can organize network share folders of the NAS. With Web File Manager, you can upload, rename, or delete files and folders in the network shares.

The screenshot shows a file manager interface with the following details:

- Address bar: admin:Qmultimedia/
- Toolbar: Includes standard file management icons like back, forward, home, and search.
- Header: "Gesamt: 3 Ordner , 0 Dateien" and a dropdown menu set to 1.
- Table view:

Name	Größe	Datum
.@_thumb	--	2009/04/13 18:07
music	--	2009/04/14 03:00
photos	--	2009/04/13 18:02
- Buttons at the bottom: "Heraufladen des Dateinamens:" (Upload file name), "Browse...", "Heraufladen" (Upload) with a green arrow icon.

### View files online

Click a file displayed on the web page. The information of the file will be displayed.

If your browser does not support the file format, a download window will pop up automatically. Download the file and you can open it on your PC.

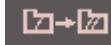
### Create folder

- i. Select a network share or folder in which you want to create a new folder.
- ii. Click (Create Folder) on the toolbar.
- iii. Enter the name of the new folder and click "OK".

### **Rename file or folder**

- i. Select a file or folder to rename.
- ii. Click  (Rename) on the toolbar.
- iii. Enter the new file or folder name and click "OK".

### **Move/copy files or folders**

- i. Select the files or folders to move or copy.
- ii. On the tool bar, click  (Move/Copy).
- iii. You can select the destination folder to which the selected files or folders are moved or copied.

### **Delete file or folder**

- i. Select a file or folder to delete.
- ii. Click  (Delete) on the toolbar.
- iii. Confirm to delete the file or folder.

To delete all files and folders, click  (Select All) and  (Delete).

### **Upload file**

- i. Open the folder to upload file to.
- ii. Click "Browse" to select the file.
- iii. Click "Upload".

### **Download file**

- i. Select a file to download.
- ii. Right click the mouse and select "Save Target As" to save the file.

### **Logout**

To exit Web File Manager, click  (Logout).

## Web File Manager Icons

Icon	Description
	Return to the parent folder
	Refresh the current page
	Return to network share list home page
	Create folder
	Rename file or folder
	Delete file or folder
	Select all
	Cancel selection
	Logout
	Full access network share folder
	Read-only network share folder
	Malfunction network share folder

# **Chapter 9    NetBak Replicator**

NetBak Replicator is a powerful program installed in user's system (Windows® OS only) for data backup. You can back up any files or folders on local PC to specified share folder on the NAS by LAN or WAN.

## **Main Functions**

### **1. Backup**

- Instant Backup

You can select files and folders on local PC and back up files to specified network share folder on the NAS immediately.

- File Filter

You can select particular file types to be excluded from backup. The system will filter all files belonging to these file types when backing up data.

- Schedule

You can specify a schedule for backing up data with this option, e.g. 12:00 every day or 05:00 every Saturday.

- Monitor

When this option is enabled, the system will upload all files or folders to the server instantly for backup when the files or folders are modified.

### **2. Restore**

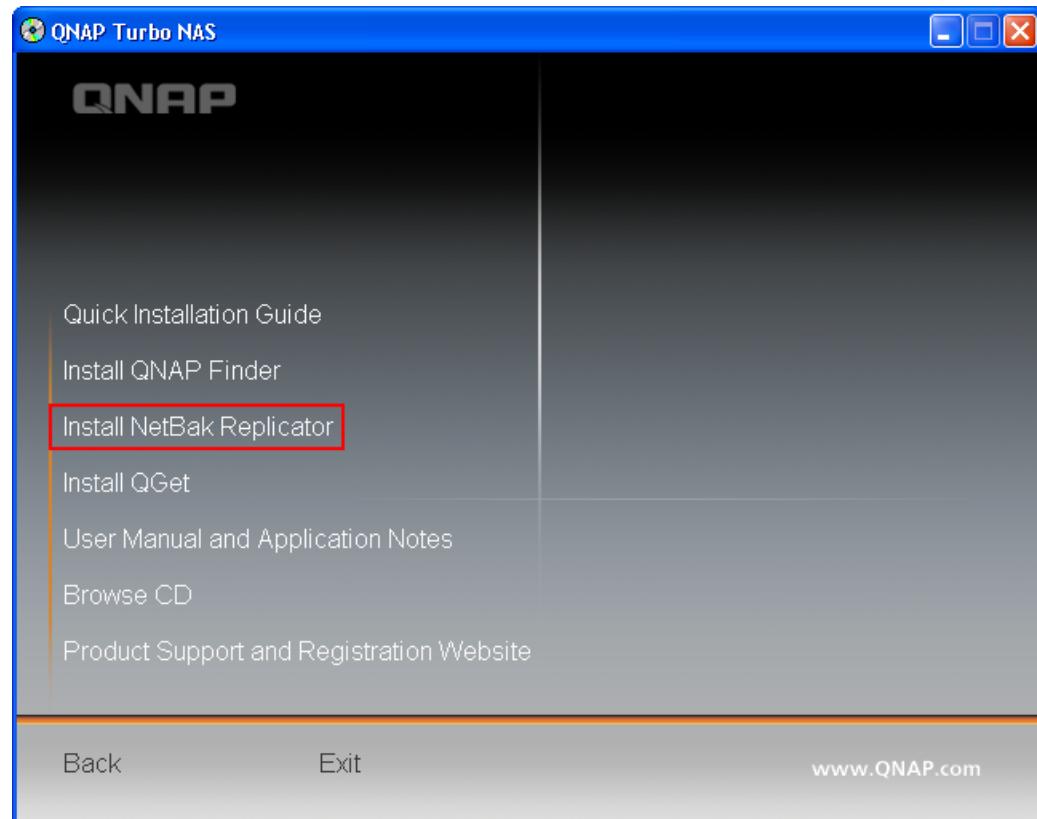
Select this option to restore backed up data to the original location of the file or to a new directory.

### **3. Log**

Enable this option to record events of NetBak Replicator, e.g. the time when NetBak Replicator starts and terminates.

## **Install NetBak Replicator**

1. Run the NAS CD-ROM. Select "Install NetBak Replicator".



2. Follow the steps to install NetBak Replicator.



3. Upon successful installation, a shortcut icon  will be shown on the Desktop. Double click the icon to run NetBak Replicator.

## Use NetBak Replicator

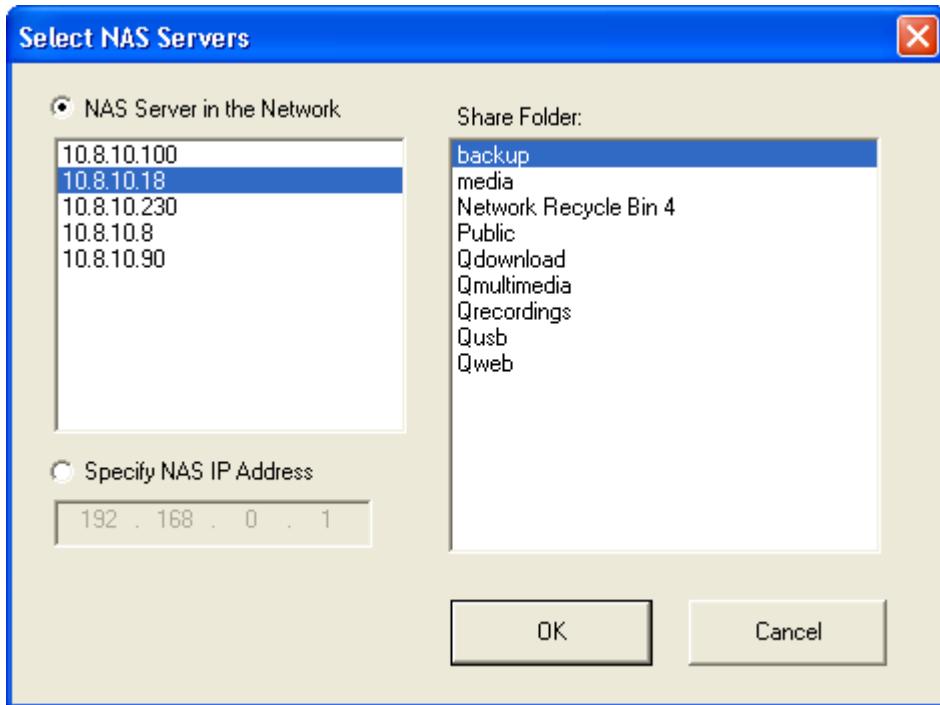
1. Before using NetBak Replicator, please login the NAS administration and go to "Access Right Management" > "Share Folders" to create a share folder for backup. Make sure the share folder is open for everyone access or you login the share folder with an authorized account or administrator by NetBak Replicator.



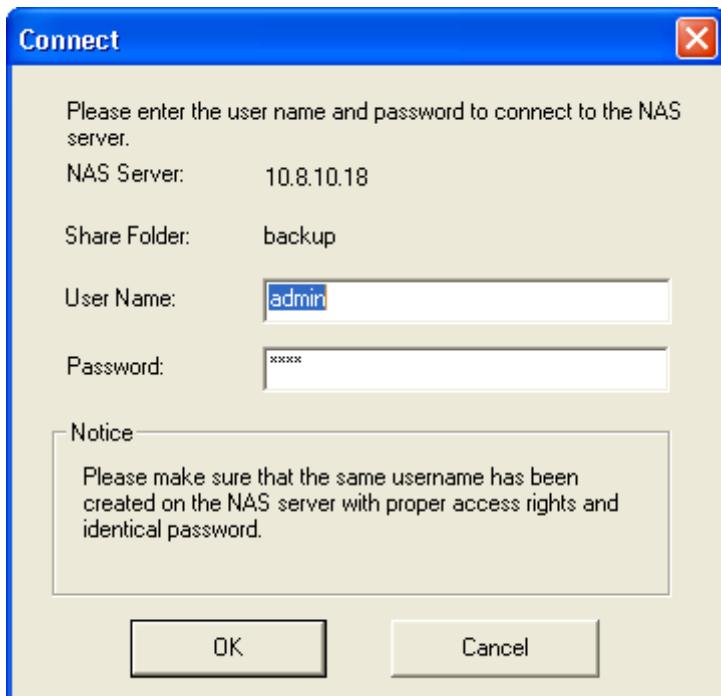
2. Run NetBak Replicator. Click All the NAS and their share folders within the network will be displayed.



3. When the following window appears, all the NAS in the LAN will appear on the left list. Select a server and a share folder on the right. NetBak Replicator also supports backup via WAN, you can enter the IP address of the NAS for data backup directly and select a share folder. Then click "OK".



4. Enter the user name and password to login the server.



5. You can start the backup procedure upon successful connection to the NAS.

## Description of Buttons on NetBak Replicator

	Open Configuration: Open a previously saved NetBak Replicator configuration.
	Save Configuration: Save the settings on NetBak Replicator. The file will be named as *.rpr
	Select All: Select all items in the window.
	Clear All: Clear selection.
	Select My Document: Select all folders in My Document.
	Open NAS Backup Folder: This button allows users to find out where the files were backed up, and check or manage the archived files manually.
	Advanced Backup: Advanced Backup allows power user to back up a single folder with more advanced options.

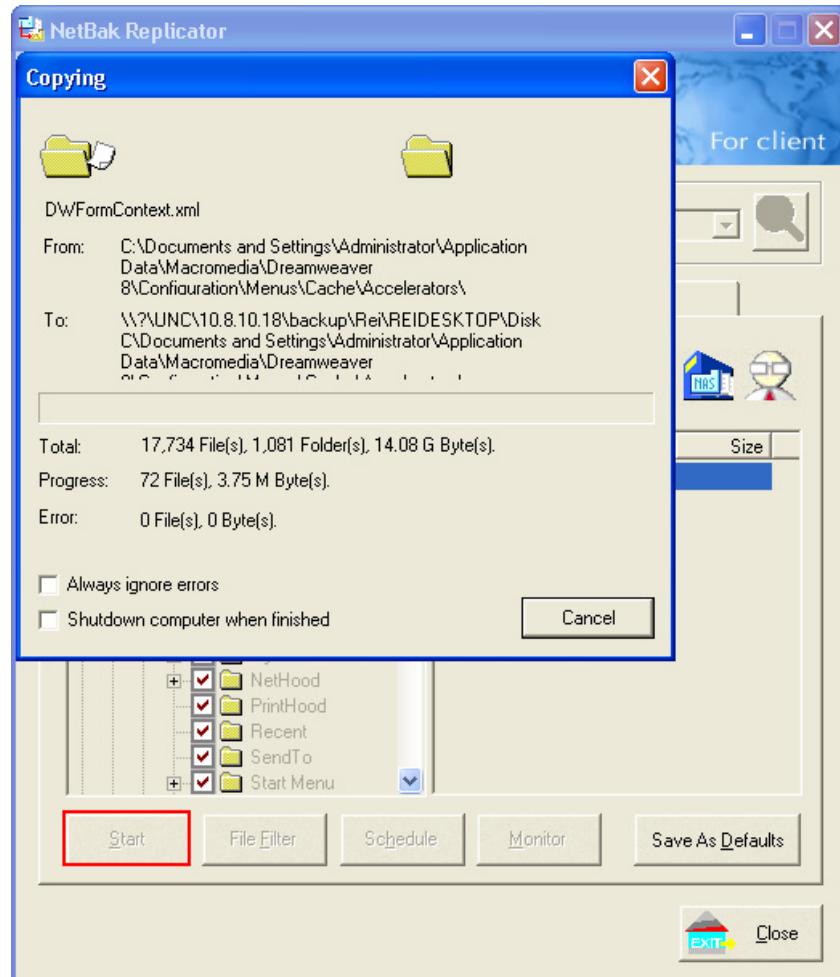
- **Backup**

Select the files and folders for backup.



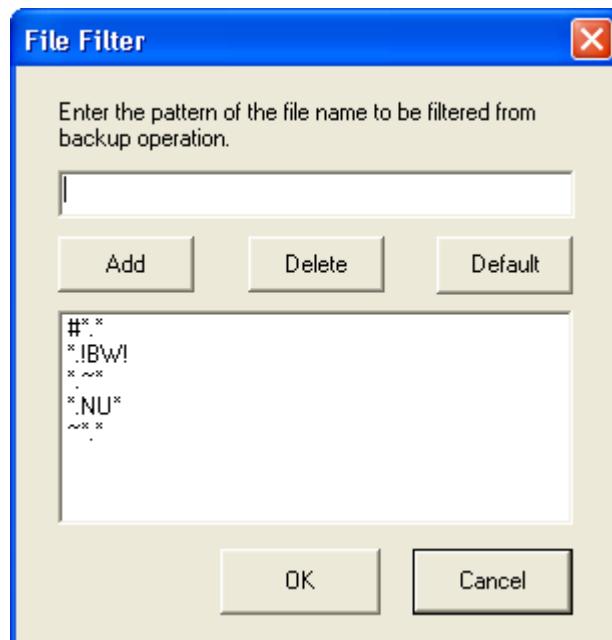
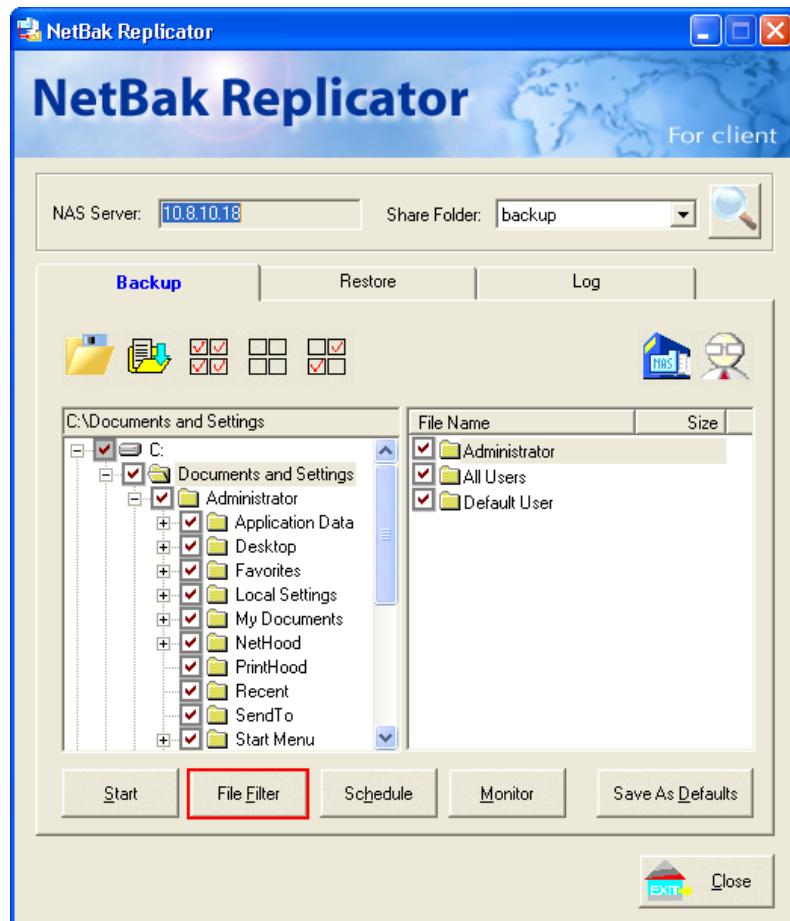
✓ Start

When you have selected the files for backup to the NAS, click "Start". The program will start to copy the selected files to the specified share folder on the NAS.



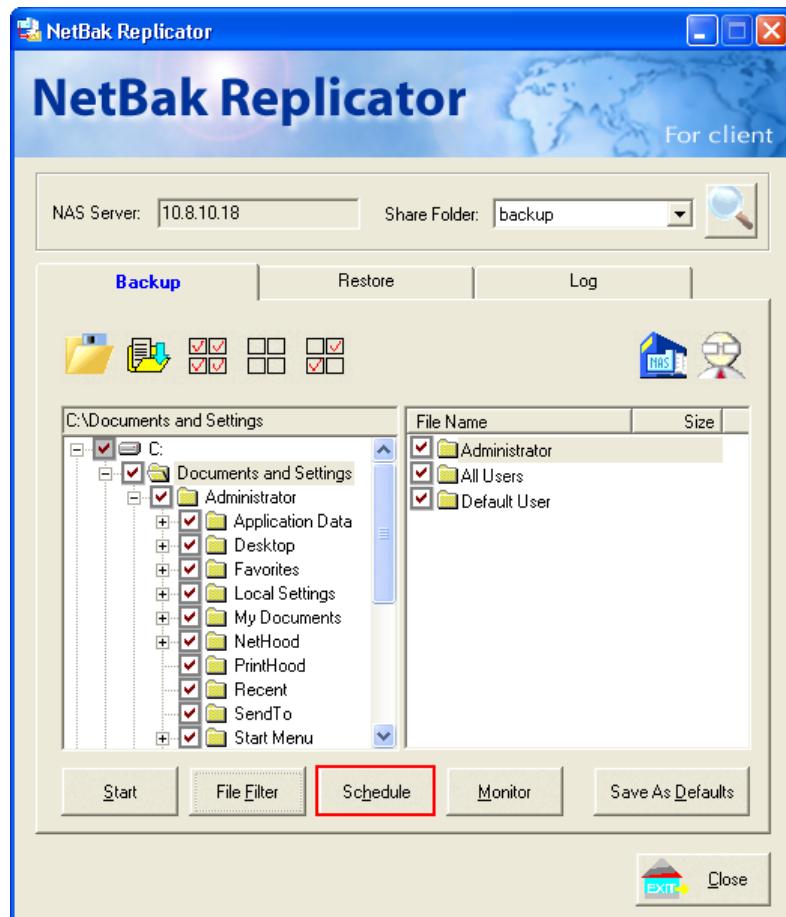
✓ File Filter

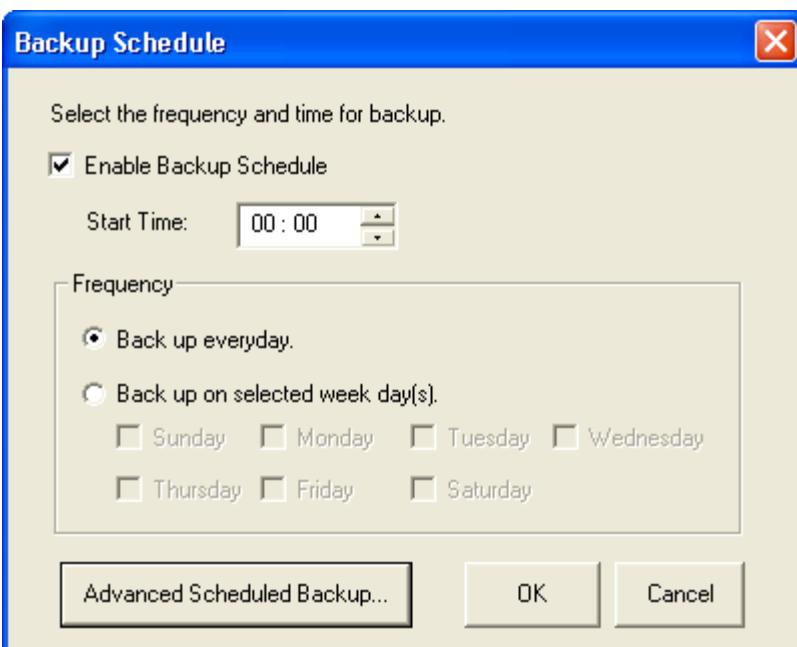
Click "File Filter" on NetBak Replicator main page to select file format to be skipped from backup. Then click "OK".



✓ Schedule

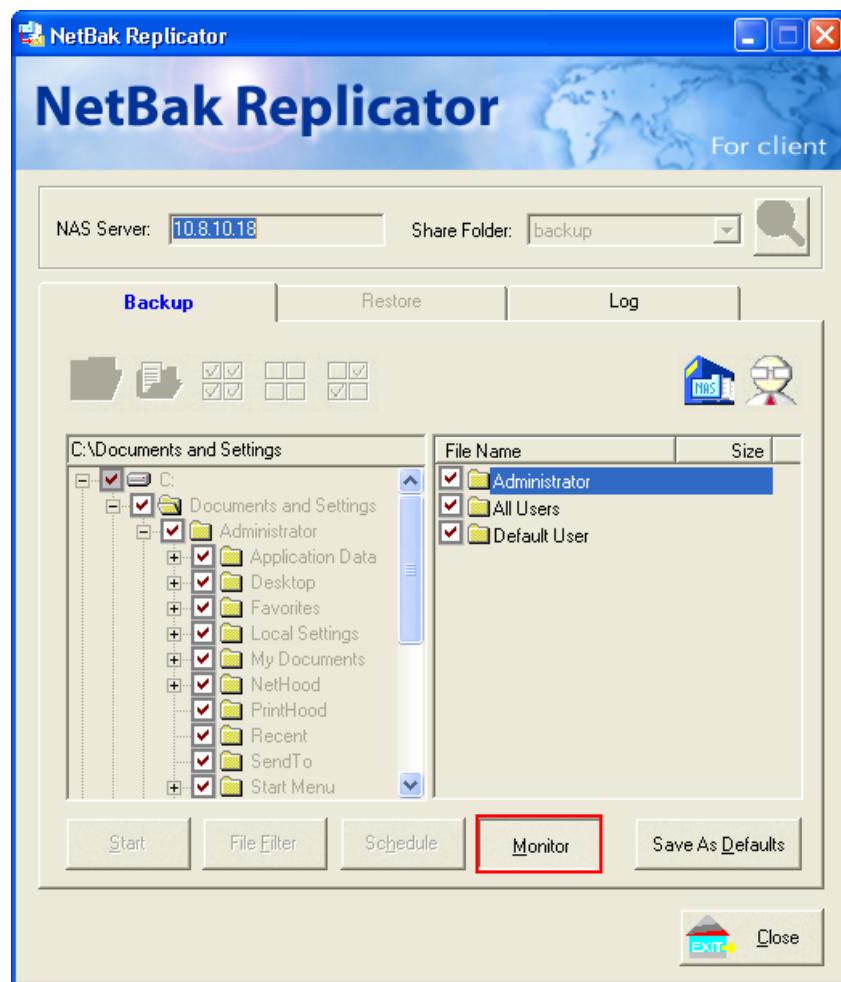
Click "Schedule" on NetBak Replicator main page. Then check the box "Enable Backup Schedule" and select the frequency and time for backup. Click "OK" to confirm.





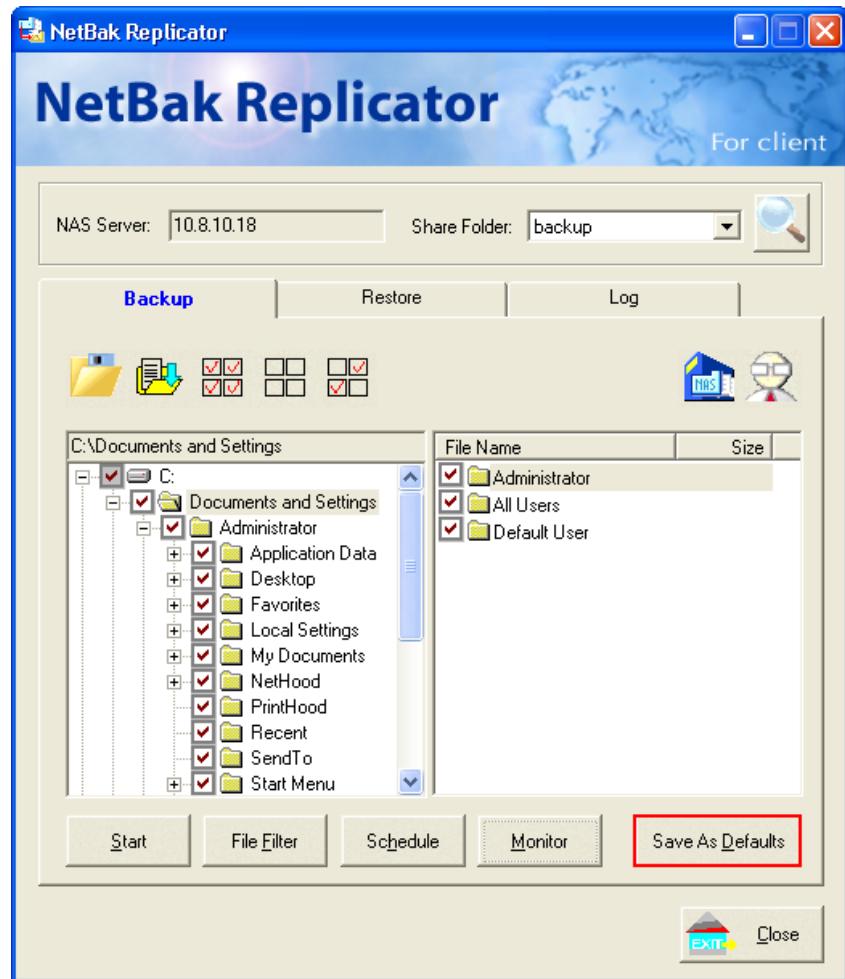
✓ Monitor

Select a folder for monitoring. When this option is enabled, the system will upload all files or folders to the server instantly for backup when the files or folders are modified. Other files will be gray and cannot be selected. Click "Monitor" again to cancel monitoring. An icon  will appear on task bar of Windows® when monitoring is in process.



✓ Initialize Configuration

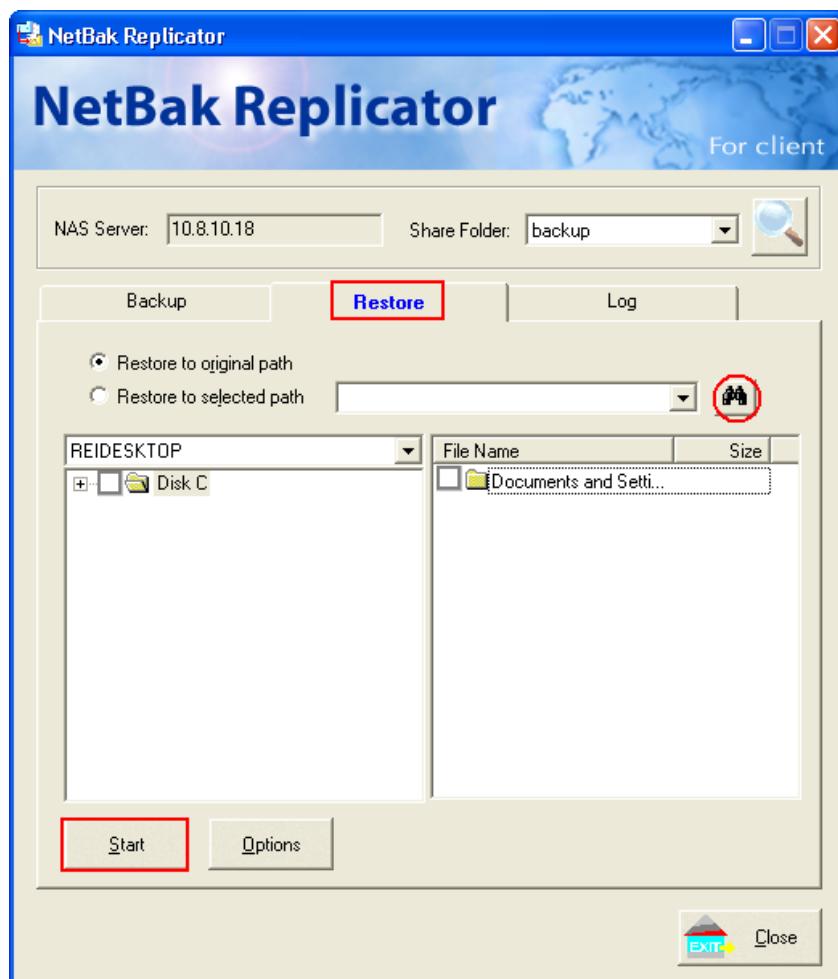
When using this function, NetBak Replicator will record all current settings of the user, including whether or not monitor function is enabled. When the user login again, this program will load the previous recorded settings for users to manage data backup.



- **Restore**

Please follow the steps below to restore files from the NAS to your PC.

- Restore to original position: Select the location that the data will be restored to.
- Select new restore position: Click  to select the directory to restore data to or select a previously chosen location from the drop-down menu.
- Select the folder(s) and sub-folder(s) for restoring data on the right list and click "Start".



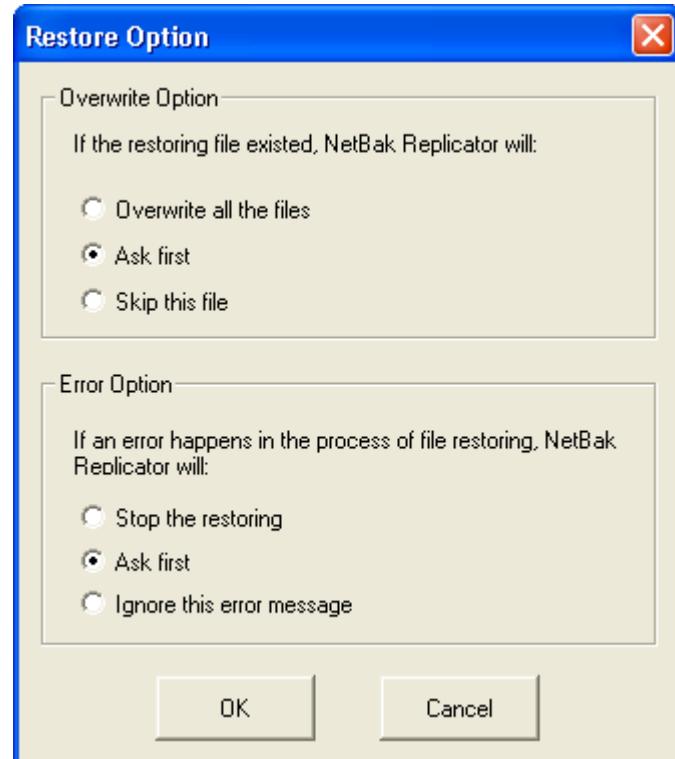
d. Option: Select recovery option and error option.

If the restoring file existed, NetBak Replicator will:

- ✓ Overwrite all the files
- ✓ Ask first
- ✓ Skip this file

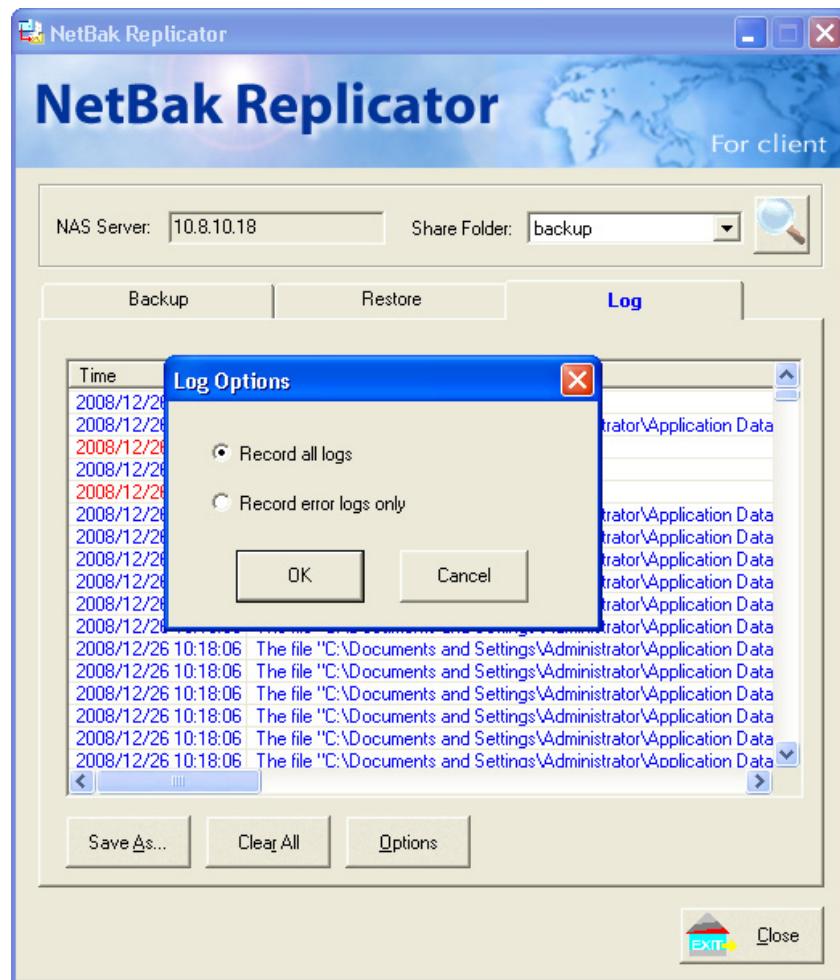
If an error happens in the process of file restoring, NetBak Replicator will:

- ✓ Stop the restoring
- ✓ Ask first
- ✓ Ignore this error message



- **Log**

- a. Save As...: To save all logs on NetBak Replicator, click this button. All logs will be saved as text file.
- b. Clear All: Click this button to clear all logs.
- c. Option: Select the type of logs to be recorded— “Record all logs” or “Record error logs only”.

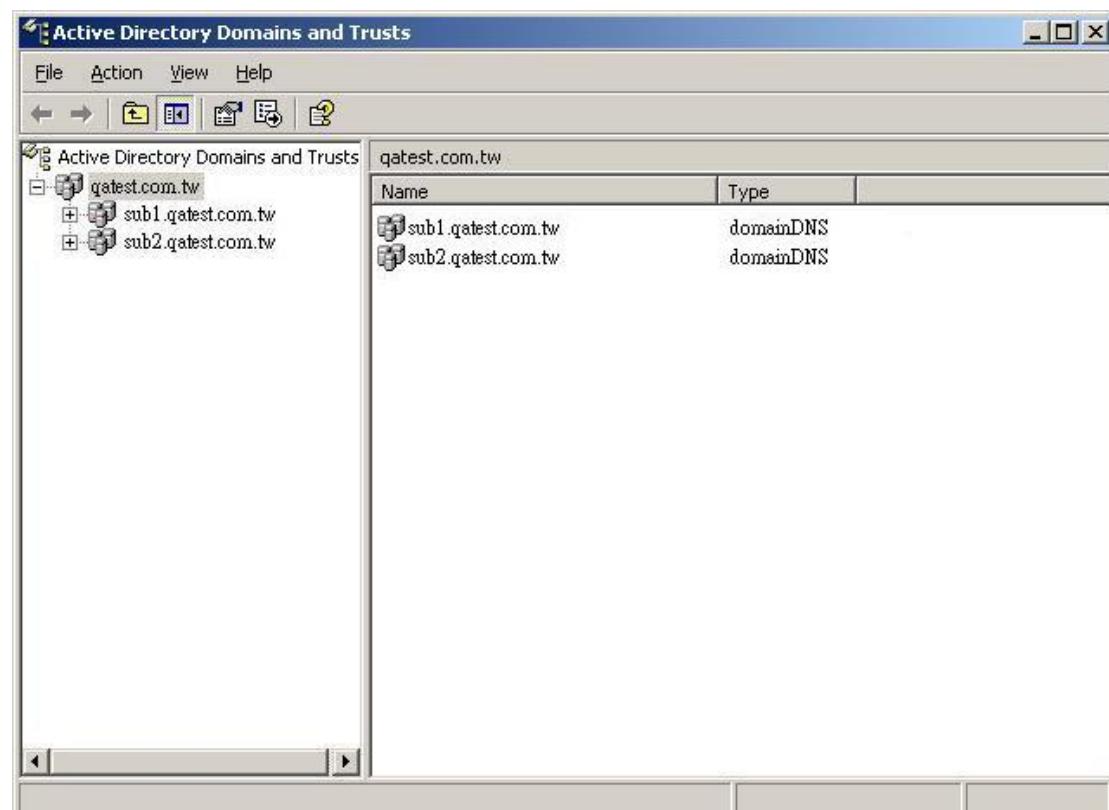


## Chapter 10 Configuring AD Authentication

The NAS supports Active Directory (AD). You can import the user accounts from Windows AD domain to the NAS. This saves your time to create users one by one.

The example below demonstrates how to use this service.

We have two domains qatest.com.tw and sub2.qatest.com.tw controlled by Windows 2003 server, and a domain sub1.qatest.com.tw controlled by Windows 2000 server.



Please make sure you have enabled the Active Directory Service on the Windows Server and check the following items:

- The NAS's DNS server setting must be assigned to AD server.
- The NAS and AD server can synchronize only if their time difference is less than 5 minutes.
- The NAS and AD server will synchronize every 5 minutes. To configure the settings manually, the NAS has to be set as standalone mode and then added to AD domain.
- After adding to AD domain, you must login as Domain\_name\Username to access Network Neighborhood. Local users of the NAS cannot access the server by Network Neighborhood.
- It is suggested to use Windows 2000 Service Pack 4, or Windows 2003 Service Pack 1.
- When the NAS is added to AD domain, the authority of "everyone" will not work, "everyone" is the default account of the NAS, but is not supported in AD domain. Therefore the authority has to be reset.
- The IP address of the AD server should be recorded in the DNS settings on the AD server.
- You must change the password of "admin" after you create "Active Directory" service on the AD server.
- The DNS server on the AD Server should have two records on it. For example, when the AD server name is 2003tc.testad.com, the records will be:

2003tc.testad.com A 192.168.1.100

Testad.com A 192.168.1.100

One is "A record" for AD server, and the other is the domain "A record" for DNS queries.

## Adding NAS to Windows Server 2003 Active Directory Domain

1. Go to "System Administration" > "Network". Enter the IP address of primary DNS server. You can inquire the AD domain via this DNS server.

Home >> System Administration >> Network      Welcome admin | Logout      English (US)

### Network

TCP / IP    DDNS

**IP Address**

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
Ethernet1+2	No	10.8.12.144	255.255.254.0	10.8.12.1	00:08:9B:B9:28:1B	100Mbps	1500		

**Port Trunking**

Port Trunking provides network load balancing and fault tolerance by combining two Ethernet interfaces into one to increase the bandwidth beyond the limits of any one single interface at the same time offers the redundancy for higher availability when both interfaces are connected to the same switch that supports 'Port Trunking'.

Enable Network Port Trunking

Select the port trunking mode from below. Please note that incompatible mode settings might cause the network interface to hang or affect the overall performance. For more information, please click [here](#).

Active Backup

**DNS Server:**

Primary DNS Server: 168.95.1.1

Secondary DNS Server: 10.8.2.9

**APPLY**

2. Go to "Network Services" > "Microsoft Networking". Enable AD Domain Member, and enter the domain name and the user name with administrator access right to that domain.

Home>> Network Services>> Microsoft Networking

## Microsoft Networking

**Microsoft Networking**

Enable file service for Microsoft networking  
 Standalone Server  
 AD Domain Member

Server Description:   
Workgroup:   
AD Server Name:   
Domain Name:   
Domain Username:   
Password:

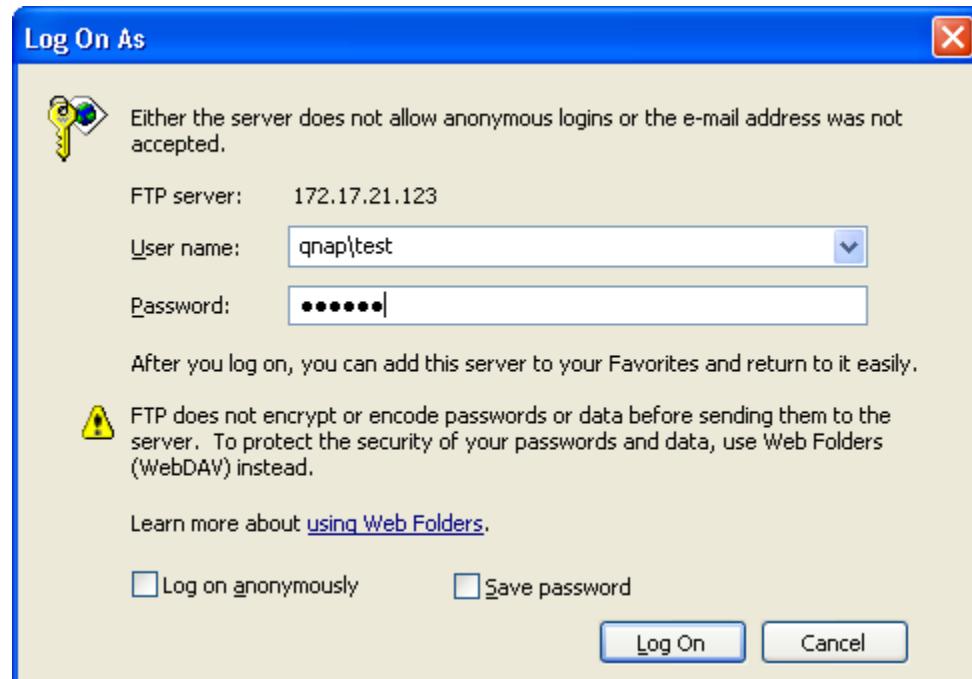
Enable WINS server  
 Use the specified WINS server  
WINS server IP address:   
 Domain Master

**Note:**

- a. Make sure that a fully qualified domain name such as qnap.com has been filled in.  
b. Make sure the user name with administrator access right to that domain.
3. Make sure the difference of your time and that of AD server is less than 5 minutes. If the time difference is larger than 5 minutes, you will not be able to add the domain member.
4. Upon successful adding of domain member, you can view the list for domain users and local users in User Management.
5. Go to Access Control in Network Share Management to configure the access control right of AD users for all available network shares.

## Using AD users to access services

To access services like FTP, Network Neighborhood, or Apple Talk with an AD user account, add **DomainName\** before the user name when logging in.



\* The step-by-step guide of adding QNAP NAS to the AD server is available on [http://www.qnap.com/pro\\_features.asp](http://www.qnap.com/pro_features.asp).

## Chapter 11 Access NAS via Linux OS

In addition to Microsoft and Mac OS, the NAS also supports Linux systems through the NFS service:

1. In Linux, run the following command:

```
mount -t nfs <NAS IP address>:/<Network Share Name>
<Directory to Mount>
```

For example, if the IP address of your NAS is 192.168.0.1 and you want to link the network share folder “public” under the /mnt/pub directory, use the following command:

```
mount -t nfs 192.168.0.1:/public /mnt/pub
```

**Note:** You must login as “root” user to initiate the above command.

2. Login as the user ID you define, you can use the mounted directory to access your network share files.

# Chapter 12 NAS Maintenance

## 12.1 Restart/ Shut down Server

Follow the steps below to restart or shut down the NAS.

1. Login the NAS. Go to "System Administration" > "Power Management".
2. Click "Restart" to reboot the server or "Shut Down" to turn off the server.

To force shut down the NAS server, press the power button for more than 10 seconds. The server beeps once and shuts down immediately.

The screenshot shows the "Power Management" section of the QNAP web interface. At the top, there are links for "Home", "System Administration", and "Power Management", along with user information "Welcome admin | Logout" and language "English". Below the header, the title "Power Management" is displayed. Under "Power Management", the "Restart/ Shutdown" tab is selected. A sub-section titled "Execute system restart/ shutdown immediately." contains two buttons: "RESTART" and "SHUTDOWN".

You can use the Finder to restart or shut down the server (admin access required).

The screenshot shows the QNAP Finder application window. The menu bar includes "Servers", "Connect", "Settings", "Tools", and "Help". The "Tools" menu is open, showing options like "Map Network Drive", "Restart Server" (which is highlighted with a red box), and "Shutdown Server". The main pane displays a list of network devices. On the right, there's a preview area showing several QNAP NAS units. A table at the bottom provides details for the selected device, which is "NAS8C3E6F".

Name	Type	IP Address	MAC Address
NAC9B67BDF9	NetBak Replicator	192.168.1.100	00-08-9B-67-BD-F9
<b>NAS8C3E6F</b>	QBack	192.168.1.119	00-08-9B-8C-3E-6F
NASAC8E60	QGet	192.168.1.409	00-08-9B-AC-8E-60
NASHP1015	VioGate Player	192.168.1.8	00-08-9B-60-84-FB
SL	VioGate Master	192.168.1.8	00-E0-4C-77-11-A6
VioStor	10.8.10.220	2.8.0 (3827)	VS-201

## 12.2 Reset Administrator Password and Network Settings

To reset the administrator password and network settings of NAS,

1. Press the reset button of the NAS for a few seconds. A beep sound will be heard.

The following settings are reset to default:

- System admin password: admin
- Network Settings/ TCP/IP Configuration: Obtain IP address settings automatically via DHCP
- Network Settings/ TCP/IP Configuration: Disable Jumbo Frame
- Network Setting/ System Port Management: 8080 (system service port)
- System Tools/ IP Filter: Allow all connections
- LCD panel password: (blank)\*

\* Applicable to models with LCD panel only.

2. Login the NAS with the default user name and password:

Default user name: **admin**  
Password: **admin**

**Note:** To reset the system by the reset button, the option "Enable configuration reset switch" in "System Administration" > "Hardware" must be activated.

The screenshot shows a web-based configuration interface for a network attached storage (NAS) device. The top navigation bar includes links for Home, System Administration, and Hardware. The main title is 'Hardware'. Below the title, there is a section titled 'Hardware' with several configuration options listed as checkboxes. The first checkbox, 'Enable configuration reset switch', is checked and highlighted with a red border. Other options include 'Enable hard disk standby mode (if no access within 5 minutes)', 'Enable light signal alert when the free size of disk is less than the value 3072 MB', and 'Enable alarm buzzer (beep sound for error and warning alert)'. The 'Enable configuration reset switch' option is described in the accompanying text as being required for system reset via the physical reset button.

## **12.3 Disk Failure or Malfunction**

When you encounter disk malfunction or failure, please do the following:

1. Record the malfunction status or error messages shown in Event Logs.
2. Stop using the failed NAS and turn off the server.
3. Contact customer service for technical support.

**Note:** The NAS must be repaired by professional technicians, do not try to repair the server yourself.

Please back up any important files or folders to avoid potential data loss due to disk crash.

## **12.4 Power Outage or Abnormal Shutdown**

In case of power outage or improper shutdown of the NAS, the system will resume to the state before it is shut down. If your server does not function properly after restart, please do the following:

1. If the system configuration is lost, configure the system again.
2. In the event of abnormal operation of the server, contact customer service for technical support.

## **12.5 System Software Abnormal Operation**

When the system software does not operate properly, the NAS automatically restarts to resume normal operation. If you find the system restarts continuously, it may fail to resume normal operation. In this case, please contact the technical support immediately.

## **12.6 System Temperature Protection**

The system shuts down automatically for hardware protection when any of the following criteria are met:

- ✓ The system temperature exceeds 70°C (158°F)
- ✓ The CPU temperature exceeds 85°C (185°F)
- ✓ The hard drive temperature exceeds 60°C (140°F)

# Chapter 13 RAID Abnormal Operation

## Troubleshooting

If the RAID configuration of your NAS is found abnormal or there are error messages, please try the following solutions:

**Note:** You must back up the important data on the NAS first to avoid any potential data loss.

1. Check that the RAID rebuilding has failed:
  - a. LED: The Status LED of NAS flashes in red.
  - b. On the “Disk Management” > “Volume Management” page, the status of the disk volume configuration is “In degraded mode”.
2. Find out the hard drive(s) that causes the RAID rebuilding failure.

You can go to “System Administration” > “System Logs” page to search for the following error message and find out which hard drive(s) causes the error.

[Error occurred while accessing Drive X.](#)

[Drive X has been removed.](#)

X refers to the number of the hard drive slot.

3. Troubleshooting

After plugging in the new hard drive (e.g., HDD 1), drive rebuilding will start. If the drive configuration fails again due to read/write error of the hard drive in the rebuilding process, identify which hard drive causes the error and follow the steps below to solve the problems.

**Situation 1:** The error is caused by the newly plugged in drive.

If the newly inserted drive (e.g., HDD 1) causes the rebuilding error, please unplug HDD 1 and plug in another new drive to start RAID rebuilding.

**Situation 2:** The error is caused by an existing drive (e.g., HDD 2) in the RAID configuration.

If the RAID configuration is RAID 1, you can do either one of the following:

- a. Back up the drive data to another storage device. Then reinstall and set up the NAS.
- b. Format the newly plugged in drive (e.g. HDD 1) as a single drive. Then back up the data on the NAS to this drive (HDD 1) via Web File Manager. Unplug the drive with errors (e.g., HDD 2). After that, insert a new drive to NAS to replace the fault drive, and execute RAID 1 migration.

**When the RAID configuration is RAID 5 or 6:** The RAID configuration is changed to degraded mode (read-only). It is recommended that you back up the data and run system installation and configuration again.

**Note:** When plugging in or unplugging a hard drive, please strictly adhere to the following rules to avoid abnormal system operation or data crash.

1. Plug in only one drive to NAS or unplug only one drive from NAS at one time.
2. After plugging in or unplugging a hard drive, wait for about ten seconds or longer until you hear two beeps from the NAS. Then unplug or plug in the next hard drive.

## Chapter 14 Use the LCD Panel

\* This section is applicable to NAS models with LCD panel only.

The NAS provides a handy LCD panel for you to perform disk configuration and view the system information.

When the NAS is started up, you will be able to view the server name and IP address:

N	A	S	5	F	4	D	E	3						
1	6	9	.	2	5	4	.	1	0	0	.	1	0	0

For the first time installation, the LCD panel shows the number of hard drives detected and the IP address. You may select to configure the hard drives.

<b>Number of hard drives detected</b>	<b>Default disk configuration</b>	<b>Available disk configuration options*</b>
1	Single	Single
2	RAID 1	Single -> JBOD -> RAID 0 -> RAID 1
3	RAID 5	Single -> JBOD -> RAID 0 -> RAID 5
4 or above	RAID 5	Single ->JBOD -> RAID 0 -> RAID 5 -> RAID 6

\*Press the "Select" button to choose the option, and press the "Enter" button to confirm.

For example, when you turn on the NAS with 5 hard drives installed, the LCD panel shows:

C	o	n	f	i	g	.	D	i	s	k	s	?		
→	R	A	I	D	5									

You can press the “Select” button to browse more options, e.g. RAID 6.

Press the “Enter” button and the following message shows. Press the “Select” button to select “Yes” to confirm.

C	h	o	o	s	e	R	A	I	D	5	?		
→	Y	e	s		N	o							

When you execute RAID 1, RAID 5, or RAID 6 configuration, the system will initialize the hard drives, create the RAID device, format the RAID device, and mount it as a volume on the NAS. The progress will be shown on the LCD panel. When it reaches 100%, you can access the RAID volume, e.g. create share folders and upload files to the folders on the NAS. In the meantime, to make sure the stripes and blocks in all the RAID component devices are ready, the NAS will execute RAID synchronization and the progress will be shown on “Disk Management” > “Volume Management” page. The synchronization rate is around 30-60 MB/s (vary by hard drive models, system resource usage, etc.).

**Note:** If a member drive of the RAID configuration was lost during the synchronization, the RAID device will enter degraded mode. The volume data is still accessible. If you add a new member drive to the device, it will start to rebuild. You can check the status on the “Volume Management” page.

To encrypt the disk volume, select “Yes” when the LCD panel shows <Encrypt Volume?>. The default encryption password is “admin”. To change the password, please login the web-based administration interface as an administrator and change the settings in “Device Configuration” > “Disk volume Encryption Management”.

E	n	c	r	y	p	t	V	o	l	u	m	e	?	
→	Y	e	s		N	o								

When the configuration is finished, the server name and IP address will be shown.

If the NAS fails to create the disk volume, the following message will be shown.

C	r	e	a	t	i	n	g	.	.	.			
R	A	I	D	5	F	a	i	l	l	e	d		

## **View system information by the LCD panel**

When the LCD panel shows the server name and IP address, you may press the "Enter" button to enter the Main Menu. The Main Menu consists of the following items:

1. TCP/IP
2. Physical disk
3. Volume
4. System
5. Shut down
6. Reboot
7. Password
8. Back

### **1. TCP/ IP**

In TCP/ IP, you can view the following options:

- 1.1 LAN1 IP Address
- 1.2 LAN1 Subnet Mask
- 1.3 LAN1 Gateway
- 1.4 LAN 1 PRI. DNS
- 1.5 LAN 1 SEC. DNS
- 1.6 Enter Network Settings
  - 1.6.1 Network Settings – DHCP
  - 1.6.2 Network Settings – Static IP\*
  - 1.6.3 Network Settings – BACK
- 1.7 Back to Main Menu

\* In Network Settings – Static IP, you can configure the IP address, subnet mask, gateway, and DNS of LAN 1 and LAN 2.

## **2. Physical disk**

In Physical disk, you can view the following options:

- 2.1 Disk1 Info
- 2.2 Disk2 Info
- 2.3 Disk3 Info
- 2.4 Disk4 Info
- 2.5 Disk5 Info
- 2.6 Disk6 Info
- 2.7 Back to Main Menu

The disk info shows the temperature and the capacity of the hard drive.

D	i	s	k	:	1	T	e	m	p	:	5	0	°	C
S	i	z	e	:	2	3	2	G	B					

## **3. Volume**

This section shows the disk configuration of the NAS. The first line shows the RAID configuration and storage capacity; the second line shows the member drive number of the configuration.

R	A	I	D	5					7	5	0	G	B
D	r	i	v	e	1	2	3	4					

If there is more than one volume, press the “Select” button to view the information. The following table shows the description of the LCD messages for RAID 5 configuration.

LCD Display	Drive configuration
RAID5+S	RAID5+spare
RAID5 (D)	RAID 5 degraded mode
RAID 5 (B)	RAID 5 rebuilding
RAID 5 (S)	RAID 5 re-synchronizing
RAID 5 (U)	RAID 5 is unmounted
RAID 5 (X)	RAID 5 non-activated

#### **4. System**

This section shows the system temperature and the rotation speed of the system fan.

C	P	U	T	e	m	p	:	5	0	°	C
S	y	s	T	e	m	p	:	5	5	°	C

S	y	s	F	a	n	:	8	6	5	R	P	M

#### **5. Shut down**

Use this option to turn off the NAS. Press the “Select” button to select “Yes”. Then press the “Enter” button to confirm.

#### **6. Reboot**

Use this option to restart the NAS. Press the “Select” button to select “Yes”. Then press the “Enter” button to confirm.

#### **7. Password**

The default password of the LCD panel is blank. Enter this option to change the password of the LCD panel. Select “Yes” to continue.

C	h	a	n	g	e	P	a	s	s	w	o	r	d
						Y	e	s	→	N	o		

You may enter a password of maximum 8 numeric characters (0-9). When the cursor moves to “OK”, press the “Enter” button. Verify the password to confirm the changes.

N	e	w	P	a	s	s	w	o	r	d	:		
												O	K

#### **8. Back**

Select this option to return to the main menu.

## **System Messages**

When the NAS encounters system error, an error message will be shown on the LCD panel. Press the “Enter” button to view the message. Press the “Enter” button again to view the next message.

S	y	s	t	e	m	E	r	r	o	r	!	
P	I	s	.	C	h	e	c	k	L	o	g	s

<b>System Message</b>	<b>Description</b>
Sys. Fan Failed	The system fan failed
Sys. Overheat	The system overheat
HDD Overheat	The hard drive overheat
CPU Overheat	The CPU overheat
Network Lost	Both LAN 1 and LAN 2 are disconnected in Failover or Load-balancing mode
LAN1 Lost	LAN 1 is disconnected
LAN2 Lost	LAN 2 is disconnected
HDD Failure	The hard drive fails
Vol1 Full	The volume is full
HDD Ejected	The hard drive is ejected
Vol1 Degraded	The volume is in degraded mode
Vol1 Unmounted	The volume is unmounted
Vol1 Nonactivate	The volume is not activated

## **Technical Support**

QNAP provides dedicated online support and customer service via instant messenger. You can contact us by the following means:

Online Support: <http://www.qnap.com/>

MSN: q.support@hotmail.com

Skype: qnapskype

Forum: <http://forum.qnap.com/>

### **Technical Support in the USA and Canada:**

Email: [q\\_supportus@qnap.com](mailto:q_supportus@qnap.com)

TEL: 909-595-2819 ext. 110

Address: 168 University Parkway Pomona, CA 91768-4300

Service Hours: 08:00-17:00 (GMT- 08:00 Pacific Time, Monday to Friday)

# **GNU GENERAL PUBLIC LICENSE**

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert

copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

## TERMS AND CONDITIONS

### 0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion

requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

#### 1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for

which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

## 2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material

outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

### 3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

### 4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

### 5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the

requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

## 6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in

accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for

use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

## 7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

## 8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

#### 9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

#### 10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give

under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

## 11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or

other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

## 12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent

obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"

WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS